Для генералов, адмиралов и офицеров
Вооруженных Сил Российской Федерации

ВОЕННАЯ МЫСЛЬ

Военная Мысль 2022 № 8 август

8

2022

ДЕНЬ ВОЗДУШНО-КОСМИЧЕСКИХ СИЛ РОССИИ

ВОЗДУШНО-КОСМИЧЕСКИЕ СИЛЫ (ВКС) – вид Вооруженных Сил Российской Федерации, приступивший к выполнению поставленных задач 1 августа 2015 года.

Воздушно-космические силы включают: рода войск — военно-воздушные силы, войска противовоздушной и противоракетной обороны, космические войска; специальные войска — воинские части и подразделения радиоэлектронной борьбы, связи, радиотехнического обеспечения и автоматизированных систем управления, инженерные, метеорологические; воинские части (подразделения) технического, тылового обеспечения и охраны органов военного управления; военно-учебные заведения и научно-исследовательские организации.

Боевые возможности ВКС ВС РФ за последние годы значительно возросли. В соединения, воинские части и подразделения ВКС поставлено большое количество новых и модернизированных единиц и комплексов вооружения и военной техники. Возросла доля современных образцов. Повысился уровень исправности авиатехники, что повлияло на увеличение показателей налета.

В ВКС ВС РФ сформированы новые управления авиационных дивизий, зенитных ракетных бригад и полков военно-транспортной авиации. Радиолокационными станциями, расположенными на территории РФ, создано сплошное поле системы предупреждения о ракетном нападении на всех воздушно-космических направлениях.

Сегодня исход военного противоборства во многом зависит от успешных действий в воздушно-космическом пространстве. Поэтому наращивание возможностей ВКС ВС РФ является одним из приоритетных направлений работы руководства государства и Вооруженных Сил Российской Федерации.

Серьезным экзаменом для ВКС ВС РФ стала специальная операция в Сирийской Арабской Республике, в которой на ротационной основе приняло участие большинство летного и инженерно-технического состава. Полученные в ходе операции навыки и знания систематизируются и используются при подготовке войск и органов военного управления, а также при разработке учебно-методических пособий.

Кроме того, с учетом опыта ведения боевых действий приняты решения по совершенствованию боевого состава и военной инфраструктуры ВКС ВС РФ. На основе полученных данных проводится модернизация самолетов и вертолетов.

В настоящее время ВКС ВС РФ демонстрируют высокую боевую и эксплуатационную готовность, а также эффективную боеспособность при выполнении поставленных задач, в том числе боевых.

Редакционная коллегия и редакция журнала «Военная Мысль» поздравляют командование, личный состав Воздушно-космических сил с профессиональным праздником! Желаем крепкого здоровья, мирного неба, благополучия и дальнейших успехов в деле укрепления обороноспособности нашей Отчизны.

ВОЕННАЯ МЫСЛЬ

№ 8 · август · 2022

ЕЖЕМЕСЯЧНЫЙ ВОЕННО-ТЕОРЕТИЧЕСКИЙ ЖУРНАЛ

АДРЕС РЕДАКЦИИ: 119160, г. Москва, Хорошёвское шоссе, 38.
РИЦ «Красная звезда», редакция журнала «Военная Мысль».
Телефоны: (495) 940-22-04, 940-12-93; факс: (495) 940-09-25.

Все публикации в журнале осуществляются бесплатно.
Журнал включен в «Перечень научных изданий Высшей аттестационной комиссии».

СОДЕРЖАНИЕ

ГЕОПОЛИТИКА И БЕЗОПАСНОСТЬ

ВОЕННОЕ ИСКУССТВО

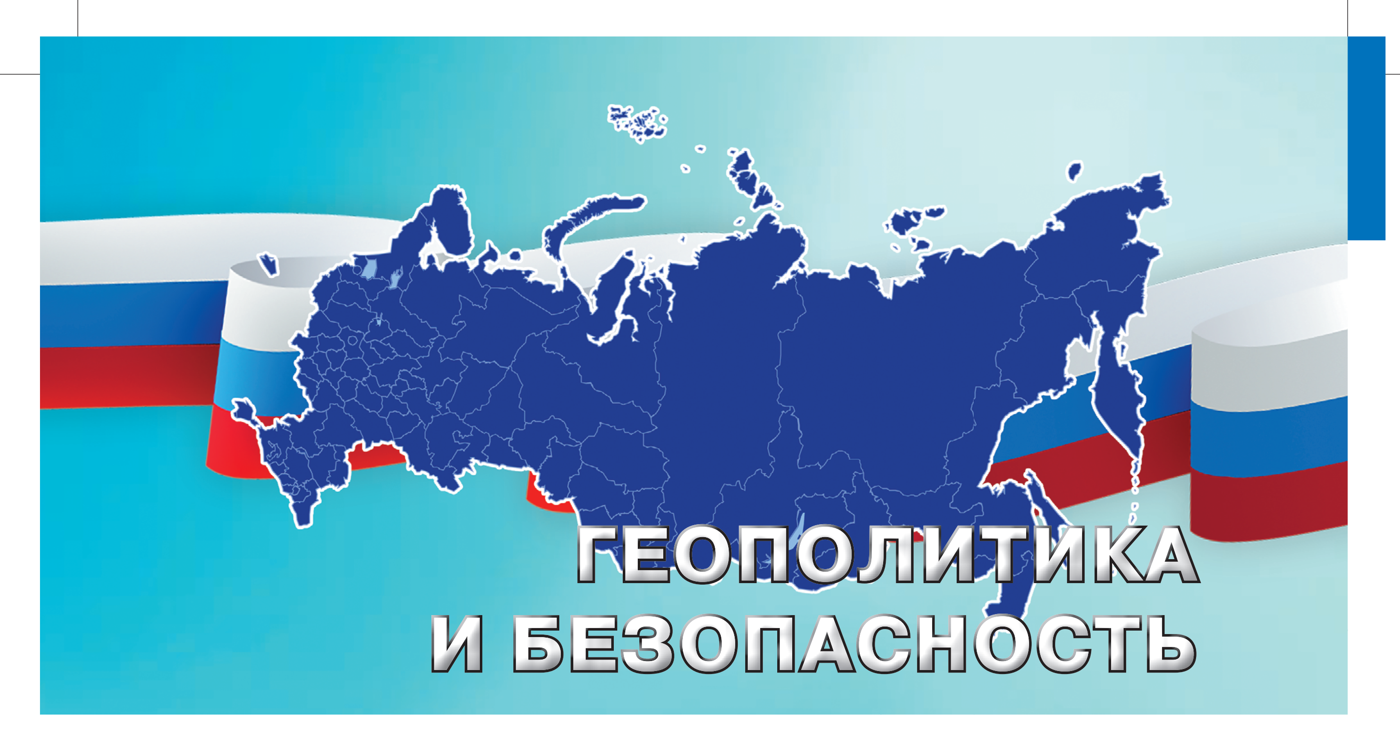
УПРАВЛЕНИЕ ВОЙСКАМИ (СИЛАМИ)

ВСЕСТОРОННЕЕ ОБЕСПЕЧЕНИЕ ВОЙСК (СИЛ)

ТЕХНИКА И ВООРУЖЕНИЕ

ОБУЧЕНИЕ И ВОСПИТАНИЕ

В ИНОСТРАННЫХ АРМИЯХ



Стратегическое сдерживание как фактор обеспечения национальной безопасности Российской Федерации

Вице-адмирал В.А. КАЛГАНОВ,
кандидат технических наук

Генерал-майор Г.Б. РЫЖОВ,
доктор военных наук

Капитан 1 ранга в отставке И.В. СОЛОВЬЁВ,
доктор технических наук

АННОТАЦИЯ

На основе анализа существующих подходов к реализации мероприятий стратегического сдерживания и результатов ранее проведенных по данной теме исследований вносятся предложения по уточнению его содержания, целей, форм, требований и принципов применительно к современным условиям. Даются рекомендации по совершенствованию организации, планирования и управления стратегическим сдерживанием на глобальном и региональном уровнях.

ABSTRACT

The paper stems from analysis of existing approaches to carrying out strategic deterrence measures and results of previous research into the subject to propose specifying its content, objectives, forms, requirements and principles with regard to present-day conditions. It offers recommendations for improving the organization, planning and control of strategic deterrence at the global and regional levels.

КЛЮЧЕВЫЕ СЛОВА

Стратегическое сдерживание, ядерное сдерживание, стратегические наступательные вооружения, сдерживающий ущерб.

KEYWORDS

Strategic deterrence, nuclear deterrence, strategic offensive weapons, deterring damage.

СТРАТЕГИЧЕСКОЕ СДЕРЖИВАНИЕ КАК ФАКТОР ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВОЕННО-ПОЛИТИЧЕСКАЯ обстановка в мире характеризуется формированием новых глобальных и региональных центров силы, между которыми обостряется борьба за сферы влияния. В результате усиливаются геополитическая напряженность, региональная нестабильность и межгосударственные противоречия, что приводит к возникновению вооруженных конфликтов в кризисных районах мира. При этом увеличивается опасность их перерастания в локальные и региональные войны, в том числе с участием ядерных держав, активно осваивающих космическое и информационное пространства как новые сферы вооруженного противоборства.

Можно констатировать, что значение военной силы как инструмента достижения субъектами международных отношений своих геополитических целей имеет устойчивую тенденцию к росту. В связи с этим на фоне реализации активной целенаправленной политики по сдерживанию западной цивилизацией поступательного развития Российской Федерации (РФ) жизненно важное значение приобретают обеспечение ее обороны и военной безопасности.

Как известно, цели обороны страны достигаются в рамках реализации военной политики, в том числе путем стратегического сдерживания и предотвращения военных конфликтов. При этом особое внимание уделяется решению таких задач, как разработка и претворение в жизнь взаимосвязанных политических, военных, военно-технических, дипломатических, экономических, информационных и иных мер, направленных на предотвращение применения военной силы в отношении РФ и поддержание на достаточном уровне потенциала ядерного сдерживания[1].

Как отмечается в Стратегии национальной безопасности РФ, поддержание стратегической стабильности относится к национальным интересам страны и является одним из «стратегических национальных приоритетов РФ»[2]. А краеугольным камнем современной стратегической стабильности является надежное и убедительное стратегическое сдерживание со стороны России.

Политика национальной безопасности РФ в области стратегического сдерживания основывается на Конституции государства, документах стратегического планирования[3,4,5] и учитывает принятые Россией международные обязательства.

Главная цель политики РФ в области стратегического сдерживания — недопущение любого вида агрессии против России и ее союзников, а в случае ее развязывания — гарантированная защита суверенитета, территориальной целостности и других жизненно важных национальных интересов российского государства и союзных стран.

Обеспечение надежного стратегического сдерживания в контексте происходящих геополитических изменений представляется задачей весьма актуальной, масштабной и значимой, что подтверждается документами стратегического планирования РФ. В основе проработки данной проблемы, по нашему мнению, лежит сложная **совокупность взаимосвязанных факторов, влияющих на эффективность стратегического сдерживания**, среди которых не только собственно военные, но и политические, экономические, информационные и другие невоенные. **К основным из них можно отнести следующие:**

• многополярный характер силовой структуры мира с размытым обликом потенциальных противников и значительной неопределенностью в реализации конкретных угроз, что затрудняет идентификацию их источников, фиксацию момента актуализации, определение целей и характера агрессивных действий противостоящей стороны[6];

• многоуровневый характер сдерживающего воздействия применительно к глобальным, региональным, блоково-коалиционным акторам (игрокам) на политической арене;

• возможность взаимного гарантированного уничтожения или войны без победителей при возникновении военного конфликта с участием ядерных держав[7];

• гибкость и комплексность манипулирования угрозами, ограничениями, демонстрацией обесценивания ожидаемых результатов агрессии, что ведет к принуждению вероятного противника к отказу от применения силовых мер при разрешении противоречий;

• деятельность в условиях активного противоборства в информационной сфере, в том числе в СМИ и в блогосфере, где участвует большое число государственных и негосударственных акторов, зачастую неподконтрольных главным сторонам конфликта[8];

• наращивание военного потенциала и попыток приобретения различных видов оружия массового поражения рядом развивающихся стран;

• развитие силовых мер на основе использования стратегических вооружений (ядерных и неядерных), нестратегического высокоточного оружия, а также оружия на новых физических принципах[9];

• наращивание несиловых мер с задействованием экономических, политических, идеологических, морально-психологических и иных механизмов сдерживания[10];

• неверные, авантюрные действия правящих элит отдельных государств по причине марионеточности, некомпетентности, необъективной оценки существующих ресурсов и возможностей, искаженной системы ценностей.

Оценивая перечисленные факторы, необходимо иметь в виду, что в **условиях многовариантности стратегического сдерживания ядерное сдерживание рассматривалось и будет рассматриваться как его основа на глобальном уровне, а невоенные меры как обеспечивающий инструмент**. Демонстрация способности при любых, самых неблагоприятных условиях осуществить ответный удар возмездия с катастрофическими последствиями для агрессора является фундаментом ядерного сдерживания.

Вместе с тем при всей важности ядерной составляющей стратегическое сдерживание должно осуществляться с задействованием всего комплекса мер, включающего как силовые, так и несиловые действия, скоординированные по целям, задачам, месту и времени. При этом в отличие от мер ядерного сдерживания применение неядерных, в том числе и несиловых средств и методов может иметь эффект за счет компенсации слабости одних из них сильными сторонами других. Это придает стратегическому сдерживанию многовариантность и гибкость реагирования на изменения обстановки в целях предотвращения неадекватного поведения одного из участников системы межгосударственных отношений.

С учетом изложенного, а также результатов анализа и обобщения документов стратегического планирования и ранее проведенных исследований **представляется целесообразным уточнить содержание, цели, формы, принципы стратегического сдерживания и требования к нему в современных условиях**.

В основе стратегического сдерживания лежит комплекс мер военного (силового) и невоенного характера, связанный с действиями по устрашению, убеждению, ограничению и принуждению. Видоизменяясь и дополняя друг друга, данные меры образуют эффективный базис сдерживающих действий, проводимых военно-политическим руководством государства в рамках единой системы, позволяющей выбирать и эффективно реализовывать тот или иной вариант сдерживания в зависимости от складывающейся обстановки и поставленных целей в мирное время, в период непосредственной угрозы агрессии, а также в условиях начавшегося военного конфликта до этапа массированного применения ядерного оружия.

Содержание стратегического сдерживания составляет комплекс мероприятий в политической, экономической, военной, информационной и других сферах, реализуемых государством в одностороннем порядке или на коалиционной основе и направленных на внушение противоборствующей стороне мысли о невозможности достижения ее военно-политических целей насильственными методами из-за неприемлемых последствий в результате ответных действий[11].

Основная цель стратегического сдерживания — недопущение силового давления и предотвращение агрессии путем убеждения потенциального противника в бесперспективности развязывания военных действий вследствие угрозы получения неприемлемого ущерба в результате ответного применения комплекса военных и невоенных мер. На наш взгляд, данную формулировку целесообразно уточнить в связи с необходимостью расширения комплексного системного влияния на объект стратегического сдерживания, дополнив ее следующим выражением: «Особое внимание в сдерживании уделяется блокированию противоречий на ранней предконфликтной стадии их развития путем воздействия на когнитивное пространство (концептосферу) потенциального агрессора».

Основываясь на законе диалектики «единства и борьбы противоположностей», можно утверждать, что ***стратегическое сдерживание — специфическая форма антагонистического взаимодействия государств*** (коалиций государств), осуществляемая путем воздействия (прямого или опосредованного) на военно-политическое руководство (ВПР) другого государства (коалиции государств) и внушения ему опасения (страха) перед последствиями военной агрессии. По сути, такое сдерживание базируется на предупреждении и устрашении ВПР потенциального агрессора о нанесении ему неприемлемого ущерба, что прямо или косвенно доводится до его сведения.

Стратегическое сдерживание базируется на следующих основных принципах:

первый — развитие и поддержание на достаточном уровне оборонной мощи государства и боевых возможностей ВС РФ с учетом экономических ограничений на уровне, обеспечивающем сдерживание любого агрессора от развязывания войны с применением всех видов оружия, включая оружие массового поражения, а в случае невозможности сдерживания — решительный разгром агрессора[12];

второй — обеспечение готовности и решимости руководства страны к применению военной организации государства, включая и ядерные силы, в соответствии с действующим российским законодательством и международными соглашениями;

третий — централизация и единство государственного и военного управления под эгидой ВС РФ федеральными, региональными органами исполнительной власти и организаци-

ями, участвующими в стратегическом сдерживании, включая планирование соответствующих мероприятий;

четвертый — постоянный мониторинг и заблаговременное выявление критических значений угроз национальной безопасности, кризисных ситуаций в опасных регионах, своевременное оповещение о них ВПР страны, принятие решения в заданные сроки по реализации мер стратегического сдерживания, в том числе на применение стратегических ядерных сил и сил общего назначения;

пятый — непрерывность мероприятий стратегического сдерживания;

шестой — гибкость и адекватность реализации мероприятий стратегического сдерживания с учетом степени опасности возникающих угроз;

седьмой — поддержание у противостоящей стороны мысли о неопределенности относительно масштабов, времени, места и других особенностей реализации мероприятий сдерживания;

восьмой — соблюдение международных обязательств в области стратегического сдерживания в отношении государств — союзников РФ;

девятый — баланс расхода ресурсов и достаточности мер воздействия на объект стратегического сдерживания пропорционально складывающейся обстановке в интересах исключения перерасхода сил и средств и недопущения чрезмерного давления на «оппонента».

Исследование трендов развития военно-политической обстановки в мире за последние 15—20 лет показывает, что **к процессу реализации мер стратегического сдерживания должны предъявляться следующие основные требования:**

- заблаговременное, многовариантное и комплексное планирование мероприятий стратегического сдерживания, обеспечивающее наиболее полное соответствие масштабов, форм и способов применения военных и невоенных мер характеру, масштабам и направленности угроз;
- взаимосвязанность мероприятий стратегического сдерживания на глобальном и региональном уровнях, сбалансированное и согласованное применение силовых и иных мер при блокировании (ликвидации) угроз военной безопасности;
- реализация всего спектра мер стратегического сдерживания по единому замыслу и плану;
- демонстрация боевых возможностей ВС РФ, в том числе ядерных, дальнобойных высокоточных средств поражения и последствий их адаптивного применения в различных условиях обстановки;
- прогнозирование реакции агрессора на угрозу или факт применения РФ стратегического оружия;
- адресность, избирательность, правдоподобность и убедительность проводимых мероприятий.

На основе анализа приведенных выше содержания, целей, форм, принципов стратегического сдерживания и требований к нему разработана концептуальная модель реализации соответствующих мероприятий в рамках его осуществления (рис.). Она представляет собой систему взглядов на применение в рамках стратегического сдерживания силовых и невоенных мер на глобальном и региональном уровнях с учетом заблаговременного воздействия на когнитивное пространство (концептосферу) субъекта сдерживания.

Главная цель политики РФ в области стратегического сдерживания — недопущение любого вида агрессии против России и ее союзников, а в случае ее развязывания — гарантированная защита суверенитета, территориальной целостности и других жизненно важных национальных интересов российского государства.

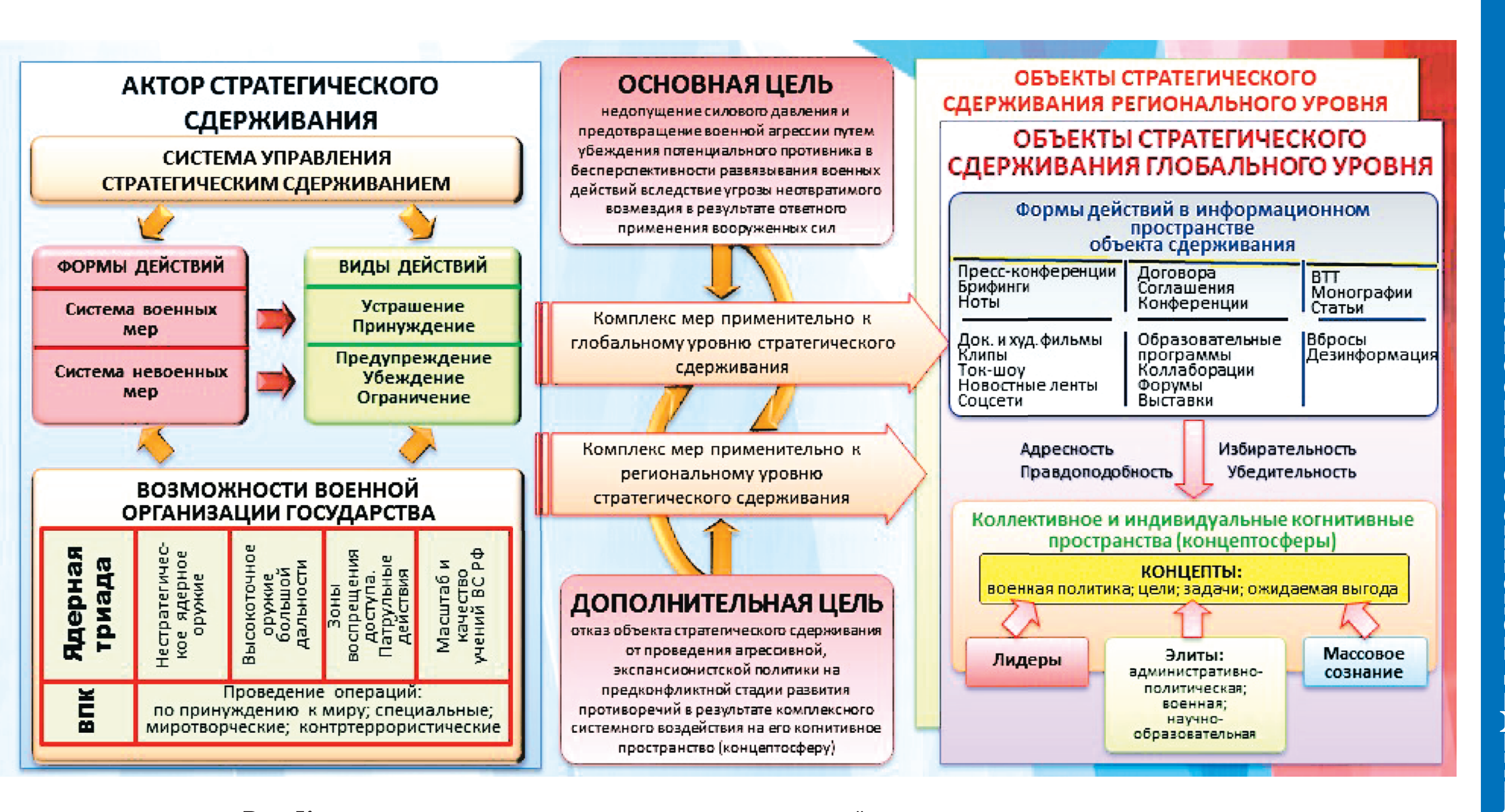


Рис. Концептуальная модель реализации мероприятий стратегического сдерживания

В данной модели с опорой на возможности военной организации государства предусматривается принятие нескольких взаимоувязанных комплексов мер, основанных на устрашении, убеждении, ограничениях и принуждении применительно к глобальному и региональному уровням стратегического сдерживания, принимая во внимание его уточненную цель. Все эти меры реализуются через соответствующие формы действий в информационном пространстве потенциального противника с адресно-избирательным воздействием на концепты, характерные для трех разновидностей когнитивных пространств субъекта стратегического сдерживания — его лидеров, элиты и массового сознания социума.

С точки зрения информационного обеспечения следует полагать, что **для качественной выработки вариантов стратегического сдерживания необходимо иметь соответствующие исходные данные**:

• список стран — объектов глобального и регионального сдерживания;

• перечень мероприятий сдерживания, относящихся к системе военных (устрашение, принуждение и др.) и невоенных (предупреждение, убеждение, ограничения и т. п.) мер и сгруппированных по видам действий;

• набор возможных действий в информационном пространстве объекта сдерживания;

• перечень концептов в области сдерживания, характерных для концептосфер потенциального противника.

Подготовка данных сведений является актуальной и весьма значимой научно-практической задачей.

Исходя из предложенной модели, центральным элементом стратегического сдерживания становится не просто устрашение угрозой уничтожения, а в первую очередь — комплексное воздействие военными и невоенными мерами на поведение ВПР потенциального противника путем целенаправленного формирования у него ожиданий относительно того, к чему приведет переход им «красных» (запретных) линий. Это позволяет предъявить объекту сдерживания убедительные свидетельства, заставляющие его поверить, что действия РФ будут решительными и адекватными его поведению. При этом стратегическое сдерживание распространяется не только на собственно военную сферу, но и на сферу возможной экономической, культурной, демографической и информационной экспансии.

На основе изложенного можно утверждать, что **в современных условиях стратегическое сдерживание, представляющее собой конкретную программу действий по реализации взаимоувязанных военных и невоенных мер, должно основываться на достаточно неплохо формализуемой когнитивной (ментальной) модели, принятой для объяснения своих действий по отношению к субъектам сдерживания**.

Вместе с тем нельзя не отметить парадокс стратегического сдерживания, который заключается в том, что, с одной стороны, оно призвано предотвратить войну, эскалацию конфликтной (кризисной) ситуации, доминирование политического соперника, а с другой — продемонстрировать реальность того или иного варианта применения военной силы.

Известно, что реализация угрозы возмездия предполагает формирование фактора определенных последствий для объекта сдерживания, которые могут носить различный характер и масштаб — от изменения мировоззрения, разрушения концептосфер и системы целеполагания лидеров, элиты, социума, разбалансировки системы принятия решений, подавления воли противостоящей стороны, осуждения и экономических санкций мирового сообщества до крупных территори-

альных, экономических и демографических потерь, вплоть до полного распада государства или ограничения его суверенитета.

Последствия стратегического сдерживания ассоциируются, как правило, с категорией «ущерб», под которым сегодня понимают главным образом ожидаемые неприемлемые потери экономического, демографического и военного потенциала в результате ответных действий. Однако, как показывает практика, возможные потери от изменения мировоззрения, разрушения концептосфер и системы целеполагания лидеров, элиты, социума, разбалансировки системы принятия решений могут в долгосрочной перспективе оказаться не менее катастрофичными и, видимо, должны также учитываться в содержании категории «ущерб».

Категория «ущерб» явно или неявно признается всеми исследователями в качестве основы стратегического сдерживания. В то же время не всякий ущерб способен удержать субъект сдерживания от прямой военной агрессии, а лишь тот, который обусловливает потери, несопоставимые с выгодами от предстоящего нападения (вторжения). Именно такой уровень (масштаб) ущерба, который обеспечивает потери противника за гранью установленной им же самим приемлемости, выражаемой, как правило, количественно, носит наименование ***сдерживающий ущерб***. Верхней границей сдерживающего ущерба является ***неприемлемый ущерб***. При этом актуальной проблемой следует считать корректное научное обоснование уровня сдерживающего ущерба, наносимого как военными, так и невоенными средствами и способами.

Отметим, что уровень сдерживающего ущерба выбирается политическим решением ВПР государства, осуществляющего стратегическое сдерживание. В частности, требования к постъядерному состоянию субъекта сдерживания, которые определяли критерии неприемлемости последствий, эволюционировали от необходимости «убийства нации» в середине прошлого века к существенному ухудшению условий функционирования государства и общества в настоящее время. При этом критерии неприемлемого ущерба связывались, с одной стороны, с уровнями поражения объекта сдерживания, а с другой — со временем его восстановления. В целом величина неприемлемого ущерба зависит от исторических, экономических, социальных, психологических и других факторов, различных для каждого объекта сдерживания[13].

Таким образом, **в основе стратегического сдерживания, опирающегося на силовой фактор и дополняемого несиловыми методами, лежит связь мер по устрашению, убеждению, ограничению, предупреждению, принуждению с возможными последствиями или сдерживающим ущербом**.

Следует констатировать, что в настоящее время в России целостная система стратегического сдерживания и ее организационные формы, предполагающие отлаженную систему взаимодействия федеральных органов исполнительной власти с Министерством обороны РФ и качественное информационное обеспечение, находится еще в стадии формирования. В ней пока не существует единого органа, осуществляющего текущее и перспективное планирование мер глобального и регионального сдерживания, а также органа, выполняющего функции оперативного управления, контроля и координации деятельности по реализации соответствующих мероприятий. В качестве таких органов могли бы выступать или существующие организационные структуры государственной власти (при наделении их соответствующими полномочиями) или вновь создаваемые структуры.

Для разрешения указанных проблем целесообразно, на наш взгляд, в документах стратегического планирования уточнить ответственность Совета Безопасности РФ в области формирования военной политики, дополнив его полномочия определением основных направлений стратегического сдерживания недружественных государств, в основе которого лежит сохранение ядерного сдерживания.

Наряду с этим, учитывая насущную необходимость, масштабность, комплексность и сложность мер стратегического сдерживания, следует проработать вопрос формирования единого органа, осуществляющего текущее и перспективное планирование соответствующих мер на глобальном и региональном уровнях. При положительном решении данной проблемы надлежит также изучить возможность и принять решение о возложении ответственности за осуществление контроля и оперативного управления реализацией мероприятий стратегического сдерживания на Национальный центр управления обороной РФ как на орган, имеющий успешный опыт координации деятельности федеральных органов исполнительной власти в сфере обороны.

При планировании стратегического сдерживания объективные уровни неприемлемого ущерба целесообразно определять с учетом возможностей стратегического и нестратегического ядерного оружия, высокоточного оружия большой дальности и невоенных мер сдерживания, а также сочетания их применения.

Для доскональной и качественной отработки вопросов планирования и реализации мер стратегического сдерживания представляется весьма насущным регулярное проведение комплексных военно-политических игр на основе базовой игровой цифровой платформы с участием как военных, так и гражданских специалистов на базе Национального центра управления обороной РФ.

ПРИМЕЧАНИЯ

[1] О Стратегии национальной безопасности Российской Федерации. Указ Президента РФ от 02.07.2021 г. № 400. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 10.04.2022).

[2] Там же.

[3] Там же.

[4] Об Основах государственной политики Российской Федерации в области ядерного сдерживания. Указ Президента РФ от 02.06.2020 г. № 355. URL: http://kremlin.ru/acts/bank/45562 (дата обращения: 10.04.2022).

[5] Военная доктрина Российской Федерации. Утверждена распоряжением Президента РФ от 25.12.2014 г. № Пр-2976. URL: https://base.garant.ru/70830556/ (дата обращения: 10.04.2022).

[6] *Хряпин А.Л., Матвейчук В.В.* Система стратегического сдерживания в новых условиях // Военная Мысль. 2010. № 1. С. 11—16.

[7] *Кокошин А.А., Есин В.И., Шляхтуров А.В.* Стратегическое сдерживание в политике нацбезопасности РФ // Независимая газета. 2021. 14, 21 октября.

[8] Там же.

[9] *Радчук А.В.* Стратегическое ядерное сдерживание: история и современность // Национальная оборона. URL: http://www.modernarmy.ru/article/242 (дата обращения: 11.04.2022).

[10] Там же.

[11] *Хряпин А.Л., Афанасьев В.А.* Концептуальные основы стратегического сдерживания // Военная Мысль. 2005. № 1. С. 8—12.

[12] Там же.

[13] *Буренок В.М, Печатнов Ю.А.* О критериальных основах ядерного сдерживания // Вооружение и экономика. 2013. № 1 (22). С. 21—30.

Концепция применения формирований войск и сил на приморских операционных направлениях Российской Федерации

Вице-адмирал В.Н. СОКОЛОВ

Полковник запаса А.В. ХАРЖАВИН,
кандидат военных наук

АННОТАЦИЯ

Представлены положения, характеризующие структуру и основное содержание концепции применения формирований войск и сил на приморских операционных направлениях Российской Федерации.

ABSTRACT

The paper gives provisions characterizing the structure and basic content of the conception of using troop and force formations in the RF maritime operational sectors.

КЛЮЧЕВЫЕ СЛОВА

Применение формирований войск и сил, приморские операционные направления РФ, концепция применения войск и сил.

KEYWORDS

Employment of troops and forces, RF maritime operational sectors, conception of using troops and forces.

ПРИМОРСКИЕ операционные направления (ОН) РФ в своем большинстве изолированы (обособлены) и значительно удалены от центра страны. Исследования[1] показали, что для успешного выполнения оперативных задач мирного и военного времени в этих особых условиях применение объединений и группировок войск и сил должно быть в составе объединенного формирования под управлением специально сформированных объединенных органов военного управления.

Данный вывод подтверждается, во-первых, опытом Крымской (1853—1856), Русско-японской (1904—1905), Великой Отечественной (1941—1945) войн. Так, в ходе последней создавались и успешно применялись единые оперативные объединения — пять оборонительных районов (Одесский, Севастопольский, Туапсинский, Новороссийский и Северный). Во-вторых, положительным опытом применения Объединенного командования войск и сил на северо-востоке Российской Федерации — современного оперативного территориального объединения Вооруженных Сил на Камчатском и Чукотском операционных направлениях[2,3]. В-третьих, взглядами военно-политического руководства США и НАТО на применение объединенных оперативных формирований различных видов вооруженных сил[4,5] под управлением объединенных командований (рис. 1).

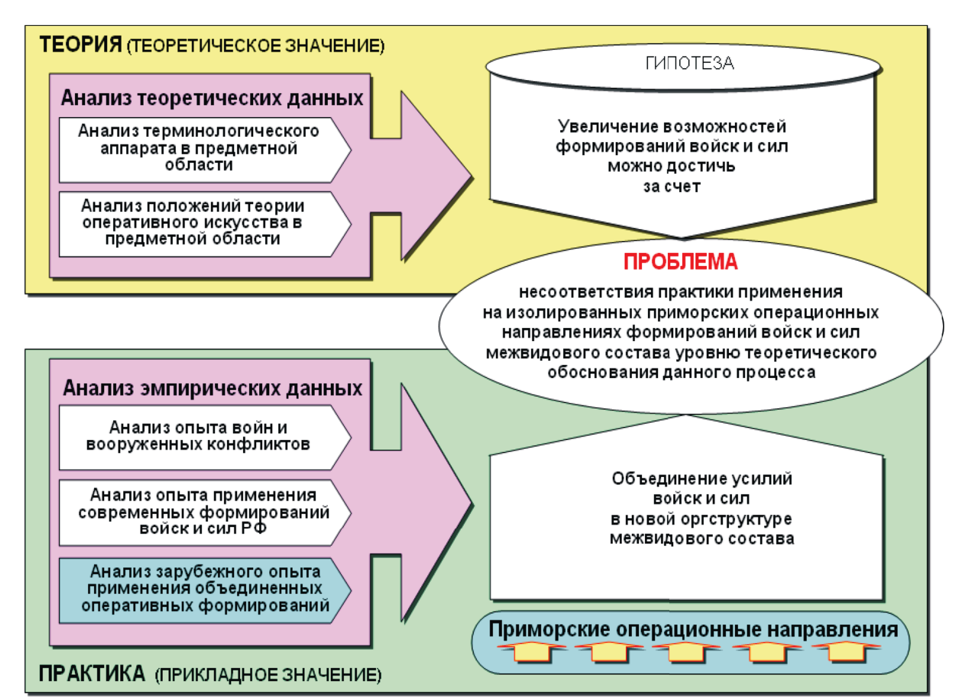


Рис. 1. Основания эмпирической и теоретической баз для объединения усилий всех сил и войск на приморских операционных направлениях в единые формирования от различных видов Вооруженных Сил

Применение объединений и группировок войск на приморских операционных направлениях РФ, включающих компоненты различных видов Вооруженных Сил, вызывает необходимость развития теоретических положений оперативного искусства в данной области. Научная проблема заключается в несоответствии степени разработки теоретических положений военного искусства в исследуемой предметной области и обоснованности применения данных формирований войск и сил на приморских операционных направлениях РФ уровню наличной практики. Для разрешения проблемы требуется разработка научно-методического аппарата в интересах наполнения концептуальных теоретических положений в исследуемой области.

В качестве теоретической основы может быть предложена концепция

применения объединенных формирований оперативного уровня войск и сил (ОФВС) на данных направлениях РФ (далее — концепция). Первоначально данная концепция построена дедуктивно-аксиоматическим методом[6].

Для обоснования корректности структуры концепции и наполнения теоретико-методологическим содержанием ее элементов разработана *методология обоснования концепции применения объединенных формирований войск и сил оперативного уровня на приморских ОН*, которая представляет собой систему строго выверенных и прошедших апробацию методов, правил, норм, разработанных моделей и методик, направленных на обеспечение адекватности концептуальных теоретических положений характеру вооруженного противоборства на данных направлениях (рис. 2).

Исходными данными в методологии являются модели действий войск и сил сторон применительно к мирному времени, периоду непосредственной угрозы агрессии и военному времени (рис. 3).

С учетом характера вооруженного противоборства, вариантов развития военно-политической обстановки и моделей действий сил сторон формируется *первый блок концепции, включающий перечень существующих и прогнозируемых военных опасностей и угроз РФ, а также вероятные сценарии военной агрессии противника и противодействия ей на приморских операционных направлениях.*

На полученной основе формируются цели и задачи войск и сил на приморских операционных направлениях. Сначала выбираются и классифицируются объекты целевого назначения по признаку отнесения их к объектам, подлежащим обороне или поражению. На объектовой базе формируется комплекс оборонительных и наступательных целей применения войск и сил на приморских направлениях применительно к мирному и военному времени. В дальнейшем методом декомпозиции целевых установок формулируются оперативные задачи, а также комплекс задач по видам обеспечения. В основе данной методической работы лежат физико-географические особенности каждого приморского операционного направления. В зависимости от классификационного вида направления[7], т. е. наличия территориальных границ с иностранными государствами, а также его географической изолированности в ходе целеполагания учитываются: то, какой противник может представлять угрозу (осуществить агрессию) — сухопутный или в виде морского десанта, степень угрозы воздушного нападения, влияния информационной борьбы и другие факторы. Таким образом, *концепция применения ОФВС оперативного уровня наполняется систематизированными по периодам применения целями и задачами войск и сил на каждом конкретном приморском операционном направлении.*

Применение объединений и группировок войск на приморских операционных направлениях РФ, включающих компоненты различных видов Вооруженных Сил, вызывает необходимость развития теоретических положений оперативного искусства в данной области. Научная проблема заключается в несоответствии степени разработки теоретических положений военного искусства в исследуемой предметной области и обоснованности применения данных формирований войск и сил на приморских операционных направлениях РФ уровню наличной практики.

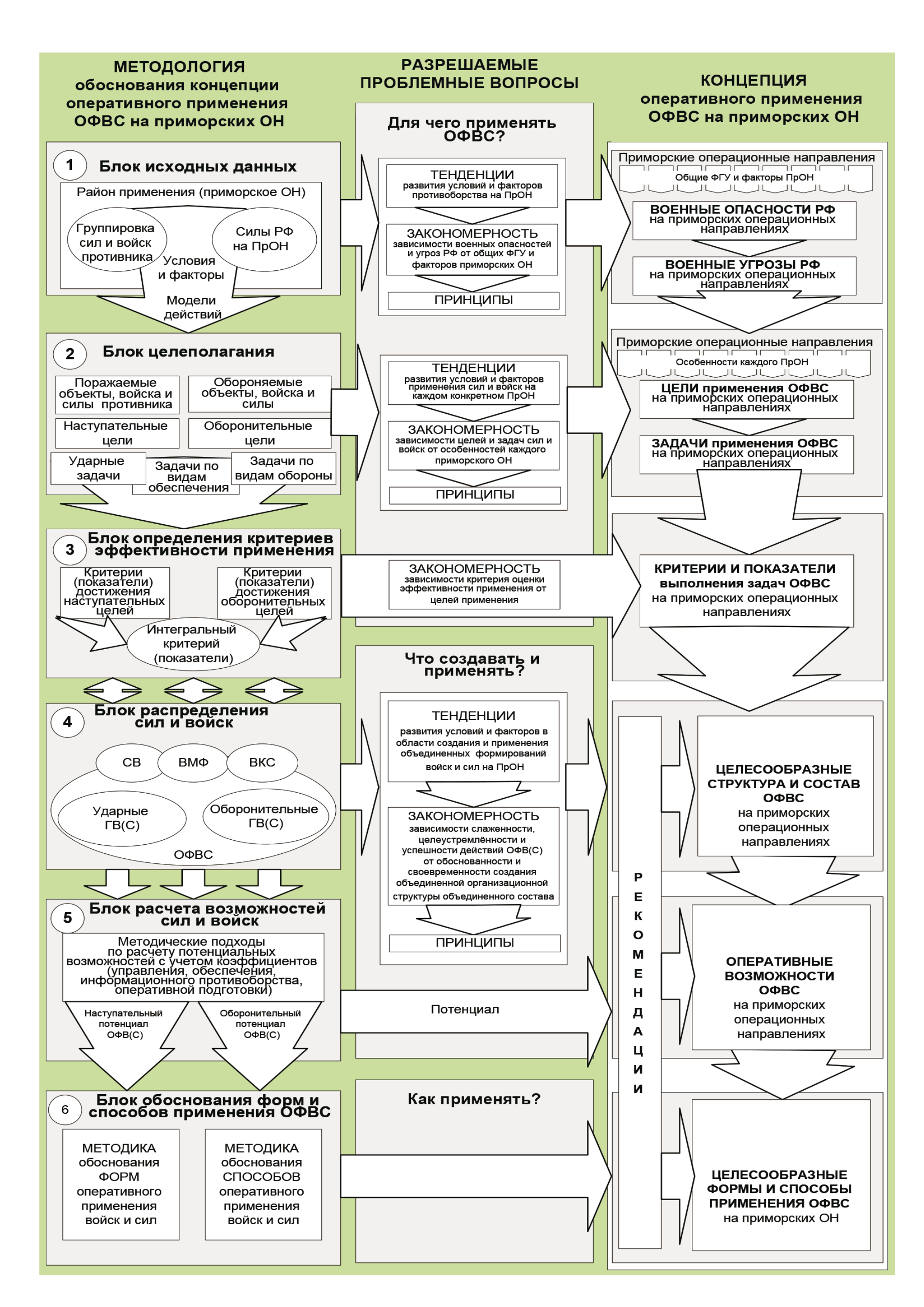


Рис. 2. Блок-схема методологии обоснования концепции применения объединенных формирований войск и сил на приморских операционных направлениях для обеспечения военной безопасности РФ

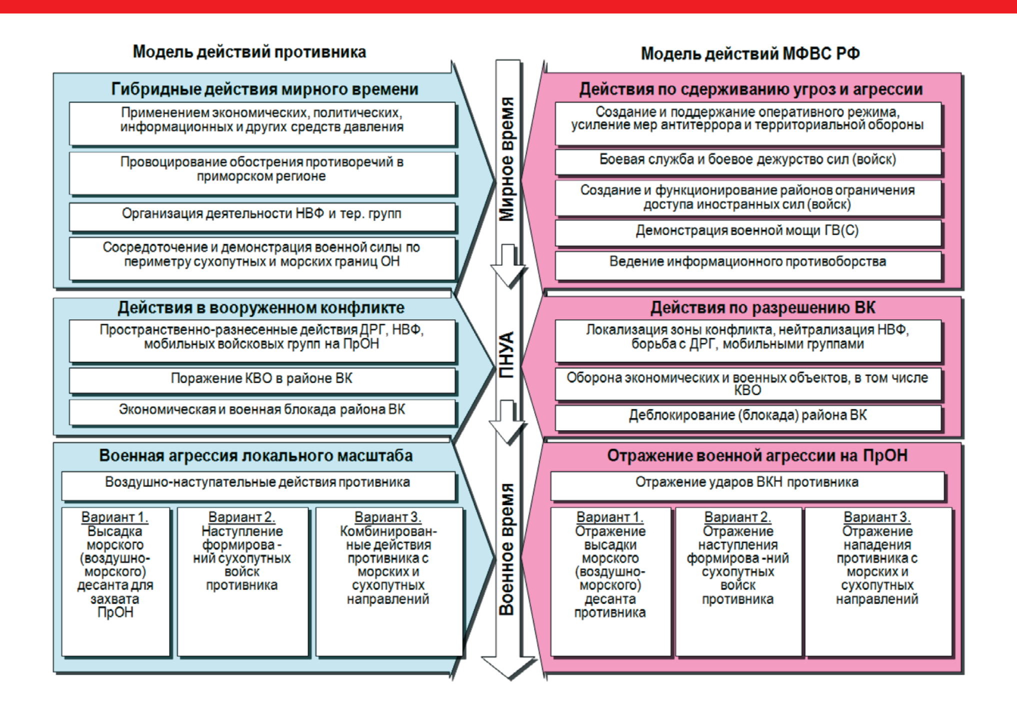


Рис. 3. Схема модели действий сил сторон на приморском операционном направлении по периодам применения (в мирное время, в период непосредственной угрозы агрессии, в военное время)

Следующим подразделом концепции является комплекс критериев, показателей и нормативов эффективности применения ОФВС. Методический подход к вопросу их определения заключается в прямой зависимости данных понятий от целей применения войск и сил и выполняемых задач[8]. Согласно данному подходу критерий эффективности соответствует уровню (степени) достижения цели с учетом вложенных затрат. Количественные значения величины выбранного критерия эффективности представляют собой показатели. Диапазон минимально допустимых и максимально достижимых показателей без перерасхода ресурса сил и средств принимается как нормативный. На полученной основе *концепция наполняется системой критериев, показателей и нормативов применительно к задачам мирного и военного времени*. Наиболее сложной теоретической задачей является определение интегральных критериев эффективности, которые отражают общую степень успешности наступательных или оборонительных действий всех составляющих ОФВС, а также их сочетание в едином комплексе одновременно проводимых действий, например в операции.

На основе вышеуказанных разделов концепции, с учетом военных опасностей и угроз, целей и задач, а также нормативных значений критериев эффективности обороны приморских направлений, определяются возможные варианты состава и структуры объединенных формирований оперативного уровня войск и сил. Методика данного поиска содержит два этапа. *На первом этапе* определяются варианты состава формирования. При этом используется метод анализа функциональных связей между видовыми элементами войск и сил в едином составе, а также положительных и негативных свойств видовых элементов формирования (рис. 4а, 4б).

Формирования Сухопутных войск

Формирования Военно-Морского Флота

Формирования Воздушно-космических сил

Взаимодополняющие связи

Обусловлены свойствами и возможностями одинакового (схожего) предназначения

Войсковая ПВО	Войска ПВО флота	Войска ПВО - ПРО
РВиА	БРАВ	ОТА

Обусловлены боевой или информационной взаимной поддержкой (дополнением)

Мотострелковые войска	МША	ОТА и АА
РВиА	МРзА	РзА

Конструктивные связи

Обусловлены конструктивно-технологическими особенностями (и сходством) ВВСТ

Концептуальные связи

Обусловлены единством целей и задач операций (боевых действий) высшего уровня

Координационно-субординационные связи

Обусловлены иерархическим положением видовых элементов в структуре МФВ(с)

***а)* сравнительный анализ функциональных связей между видовыми элементами войск и сил в составе единого объединения (группировки) на приморском операционном направлении**

***б)* анализ видовых свойств положительного и негативного характеров, учитываемых при определении вариантов состава объединенного формирования войск и сил оперативного уровня на приморском направлении**

Рис. 4. Сравнительный анализ функциональных связей между видовыми компонентами войск и сил в объединенном составе, а также анализ положительных и негативных свойств видовых элементов формирования

Для обоснования корректности структуры концепции и наполнения теоретико-методологическим содержанием ее элементов разработана методология обоснования концепции применения объединенных формирований войск и сил оперативного уровня на приморских ОН, которая представляет собой систему строго выверенных и прошедших апробацию методов, правил, норм, разработанных моделей и методик, направленных на обеспечение адекватности концептуальных теоретических положений характеру вооруженного противоборства на данных направлениях.

На втором этапе определяется организационная структура формирования войск и сил. Анализ возможных видов подчинения позволяет определить их степень приоритетности (прямое подчинение, придание, оперативное подчинение, поддержка) с использованием метода анализа иерархий[9]. На этой основе определяются целесообразные варианты структуры формирования войск и сил. Обобщение полученных данных позволяет *сформировать для концепции типовые варианты состава и структуры объединенного оперативного формирования войск и сил, адаптированные под условия применения их на приморских направлениях* с учетом данных предыдущих блоков.

В соответствии с указанной методологией для полученных вариантов состава и структуры ОФВС осуществляется расчет его оперативных возможностей, т. е. определяются оборонительный и наступательный потенциалы, которые соизмеряются с нормативными показателями.

В качестве научной основы для выполнения интегральной оценки оперативных возможностей формирования в едином функциональном комплексе используется общий логико-вероятностный метод. Он позволяет учесть систему дифференциальных уравнений Колмогорова, но не в выражении состояний, как это принято в марковских моделях, а в отражении событийных переходов. Строится схема функциональной целостности ОФВС и выполняется аналитическая работа по составлению логических уравнений, без решения систем алгебраических или дифференциальных уравнений. Символьно-лингвистическая форма отражения процесса применения структурно-сложной боевой системы выражается в виде вероятностной математической модели расчетов[10]. Событийное представление систем позволяет путем визуального логического анализа подсистем, связей между ними доказательно подтвердить корректность детального отображения и адекватность модели в целом ее графическому или вербальному прототипу.

На основе данного метода построена метамодель применения объединенных оперативного формирования войск и сил в условиях противодействия противника, ее вариант представлен в схематическом виде (рис. 5).

Расчетная метамодель позволяет определять потенциал функционирования данного формирования войск и сил, с учетом работы его взаимосвязанных подсистем: исполнительной (ударной и оборонительной), управления, информационного противоборства, обеспечения и оперативной подготовки. Он может быть выражен в вероятностной форме в виде многочлена функции:

$$P_C = p\{Y_C\} = p(\{p_i q_i\}, i = 1,2,\ldots,H) = \sum^{M}(зн_j)\prod_{i \in K_j}(p_i, q_i). \quad (1)$$

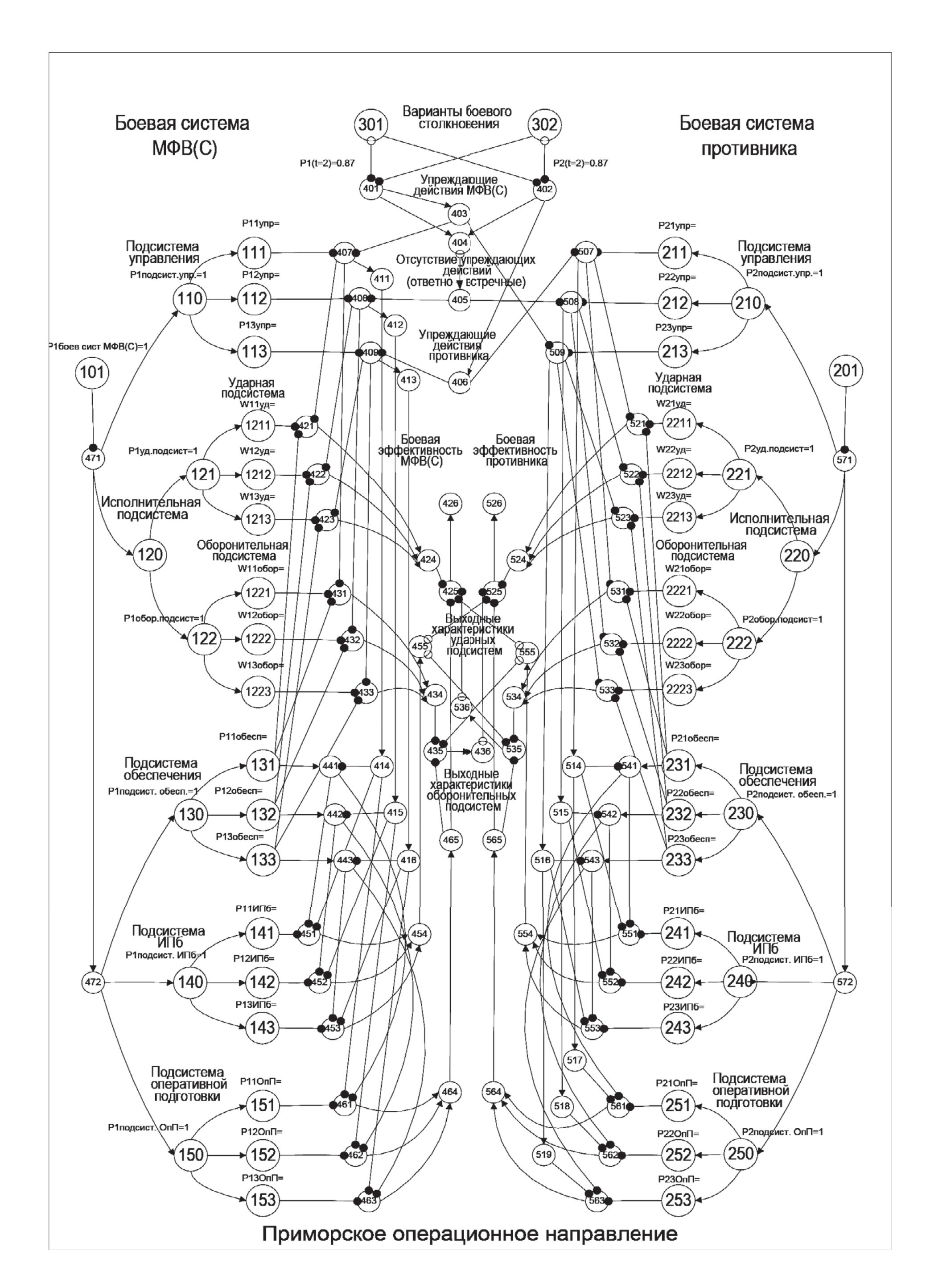


Рис. 5. Схема метамодели применения формирования войск и сил в условиях противодействия противника (вариант, полученный с использованием общего логико-вероятностного метода)

По физическому смыслу вероятность P_C определяет возможность реализации исследуемой системой заданного логического критерия Y_C ее функционирования. В теоретико-вероятностном смысле выражение (1) является законом распределения значений критерия функционирования всей системы. В математическом смысле данное выражение представляет собой правило комплексирования частных параметров функционирования подсистем ОФВС, т. е. композиции элементарных законов распределения p_i, $q_i = 1 - p_i$, в общесистемную вероятностную характеристику $P_C = p\{Y_C\}$.

Во всех случаях вероятностная функция (1) определяет правило (алгоритм) вычисления вероятности P_C сложного события Y_C, состоящего из произведений (конъюнкций), сумм (дизъюнкций) и дополнений (инверсий) составляющих его простых (элементарных) случайных событий $\tilde{x} = \{x_i, \bar{x}_i\}$, собственные вероятностные параметры p_i и $q_i = 1 - p_i$ которых известны (определены в ходе моделирования с использованием методического аппарата)[11].

Данный методический подход позволяет учесть степень влияния различных факторов функционирования подсистем объединенного оперативного формирования войск и сил на общий его потенциал. Например, максимальный учет факторов, влияющих на работу подсистем управления и оперативной подготовки, может повлиять на качество организации процесса применения. А учет работы подсистем обеспечения и информационного противоборства, как правило, отразится на уровне создания благоприятных условий для действий своих сил, а также условий, затрудняющих действия сил противника (рис. 6).

Учет влияния функционирования подсистем в объединенном составе осуществляется методом моделирования, количественно оценивается и выражается соответствующими расчетными коэффициентами. В ходе моделирования работы подсистем выявляются те факторы, которые

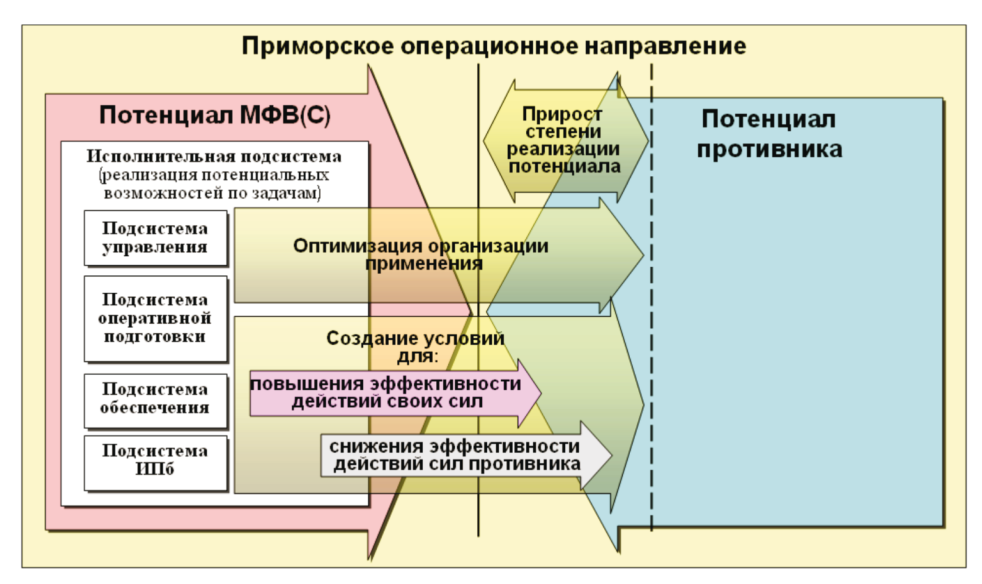


Рис. 6. Схема модели влияния факторов функционирования подсистем объединенного оперативного формирования войск и сил в интересах достижения синергетического эффекта

принимаются для учета в методическом аппарате определения показателя возможностей (потенциала) данного формирования войск и сил.

Выполненные *оценки позволяют наполнить концепцию обоснованными данными о его потенциальных возможностях.*

Сравнение полученного потенциала с нормативными требуемыми показателями может привести к выводу о том, что состав и структура формирования войск и сил удовлетворяют предъявляемым требованиям. В случае недостающего потенциала могут быть два варианта. Первый — нарастить его состав до требуемого уровня. Второй — оптимизировать процесс применения за счет выбора или разработки целесообразных форм и особенно способов применения формирования войск и сил.

Обоснование форм и способов их применения в заключительном блоке методологии представляет собой выбор (разработку) системы форм применения в различные периоды времени, а также перечня базовых способов действий в интересах обороны РФ в условиях изолированных и обособленных приморских направлений.

В зависимости от классификационного вида направления, т. е. наличия территориальных границ с иностранными государствами, а также его географической изолированности в ходе целеполагания учитываются: то, какой противник может представлять угрозу (осуществить агрессию) — сухопутный или в виде морского десанта, степень угрозы воздушного нападения, влияния информационной борьбы и другие факторы.

Научным методом при определении форм применения данных формирований войск и сил может быть избран сравнительный анализ всех известных форм применения объединений и группировок ВС РФ, их соотнесение с условиями приморских операционных направлений и адаптация к ним. При этом форма рассматривается как избранная организация действий войск и сил, включающая ряд признаков, характеризующих *внешние (организационные) рамки процесса применения и общее его наполнение.* Это прежде всего: возможный перечень и объем выполняемых задач; пространственно-временные показатели действий; привлекаемый состав сил и войск; боевое напряжение, а также избранная структура управления (руководства) силами. Исходя из условий возможной оперативной обстановки, моделей действий войск и сил сторон, по указанным признакам *в концепции выстраивается система форм применения объединенного оперативного формирования войск и сил мирного и военного времени.*

При определении целесообразных способов действий войск и сил на приморских ОН необходимо исходить из того, что собой представляет способ и в чем его отличие от понятия «форма» применения. Оперативный способ — это порядок действий сил и войск. При этом понятие «порядок» толкуется, во-первых, как пространственное распределение усилий, во-вторых, как последовательность, очередность действий, т. е. распределение усилий во времени. В отличие от формы применения оперативный способ характеризуется конкретным внутренним наполнением процесса применения. Методика разработки и обоснования способов оперативного применения имеет целью *максимизировать реализацию потенциала объединенного оперативного форми-*

рования войск и сил в специфических условиях обособленных (изолированных), удаленных от метрополии приморских операционных направлений. Методика предполагает следующий порядок действий:

во-первых, при оценке исходных данных выявляются сильные и слабые стороны своих сил и сил противника, а также физико-географические и другие факторы приморских ОН, способствующие либо затрудняющие выполнение задач;

во-вторых, исходя из полученных данных, сопоставляются общее и по направлениям соотношения сил сторон, связанные с этим возможные преимущества и недостатки;

в-третьих, определяется «схема—идея» способа, в основу которой могут быть положены отдельные принципы военного искусства или их сочетание, основанные на закономерностях вооруженной борьбы в данных обособленных условиях[12];

в-четвертых, «схема—идея» наполняется целесообразными пространственно-временными параметрами действий сил (войск), их оперативным построением, маневром в ходе выполнения задач, порядком поражения противника, тем самым формируется способ как «схема—действия»[13];

в-пятых, завершающим шагом разработки способа оперативного применения является дополнение «схемы— действия», которая представляет собой функционирование исполнительной подсистемы, мероприятиями подсистем управления, обеспечения, а также информационного противоборства, оперативной подготовки, что позволит окончательно сформировать способ применения ОФВС оперативного уровня и довести его до «схемы—организации»[14].

В итоге обобщения полученных результатов работы по данной методике *формируются и наполняют концепцию базовые варианты способов применения формирований войск и сил для типовых условий обстановки*, полученных при классификации приморских операционных направлений РФ.

При определении целесообразных способов действий войск и сил на приморских ОН необходимо исходить из того, что собой представляет способ и в чем его отличие от понятия «форма» применения. Оперативный способ — это порядок действий сил и войск. При этом понятие «порядок» толкуется, во-первых, как пространственное распределение усилий, во-вторых, как последовательность, очередность действий, т. е. распределение усилий во времени. В отличие от формы применения оперативный способ характеризуется конкретным внутренним наполнением процесса применения.

Таким образом, концепция применения объединенных оперативных формирований войск и сил на приморских операционных направлениях, построенная на рассмотренной теоретико-методологической основе (см. рис. 1):

- имеет логически выстроенную структуру, основанную на комплексе военных опасностей и угроз, моделей действий сил сторон;
- наполнена методически обоснованным содержанием, направленным на объединение усилий видовых составных частей в единой структуре объединенного оперативного формирования, функционирующего под управлением объединенного командования;
- позволяет разрешить проблемные вопросы оперативного искусства в предметной области применения объединенных оперативных форми-

В итоге обобщения полученных результатов работы по данной методике формируются и наполняют концепцию базовые варианты способов применения формирований войск и сил для типовых условий обстановки, полученных при классификации приморских операционных направлений РФ.

рований войск и сил оперативного уровня на приморских операционных направлениях РФ в целях их обороны — что применять, зачем применять, как применять;

• может составить теоретическую основу для уточнения нормативных документов в предметной области применения войск и сил на приморских операционных направлениях в объединенном составе;

• встраивается в систему теоретических положений оперативного искусства и развивает методологию исследования проблем в части, касающейся области применения объединенных группировок войск и сил в мирное и военное время[15].

ПРИМЕЧАНИЯ

[1] *Харжавин А.* Ретроспективный анализ опыта оперативного применения межвидовых формирований Вооруженных Сил России на приморских направлениях / Сборник научных трудов СПб.: ВУНЦ ВМФ «ВМА». Ч. 2. 2019. С. 193—206.

[2] *Егоров В.* Военно-политическая обстановка в Балтийской морской зоне в конце XX века и ее перспективы в XXI веке // Морская индустрия. 1999. № 4 (9). URL: http://mi32.narod.ru/04-99/egorov.html (дата обращения: 11.04.2022).

[3] *Липилин С.* Перспективы Командования Войск и Сил на Северо-Востоке России // Красная звезда. 2015. 17 сентября. URL: https://oko-planet.su/politik/politikarm/293260-perspektivy-komandovaniya-voysk-i-sil-na-severo-vostoke-rossii.html (дата обращения: 08.02.2022).

[4] *Печуров С.* «Объединенность» в системе управления ВС США // Зарубежное военное обозрение. 2002. № 1. С. 2—8.

[5] *Печуров С.* К вопросу о создании постоянных штабов объединенных оперативных формирований ВС США // Зарубежное военное обозрение. 2005. № 1. С. 8—12.

[6] *Соколов В.Н., Харжавин А.В.* Закономерности и принципы оперативного применения формирований войск и сил на приморских операционных направлениях Российской Федерации // Военная Мысль. 2022. № 5. С. 32—45.

[7] Там же.

[8] *Абчук В.А., Матвейчук Ф.А., Томашевский Л.И.* Справочник по исследованию операций. М.: Воениздат, 1979.

[9] *Саати Т.* Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1989. 316 с.

[10] *Поленин В.И.* и др. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства: монография / В.И. Поленин, И.А. Рябинин, С.К. Свирин, И.А. Гладков. СПб.: НИКА, 2011.

[11] Там же.

[12] *Соколов В.Н., Харжавин А.В.* Закономерности и принципы оперативного применения…

[13] *Мешков О.К.* Теория способов оперативного применения флотов в вооруженной борьбе на море: дис. … доктора военных наук. СПб., 1999.

[14] Там же.

[15] Приказ Министерства образования и науки РФ от 28.07.2021 г.

Методологические основы теории и практики применения робототехнических комплексов военного назначения

Генерал-майор Р.О. НОГИН

Полковник запаса А.В. ХАЧАТРЯН, кандидат военных наук

Подполковник А.В. ШИЛОНОСОВ, кандидат педагогических наук

АННОТАЦИЯ

Представлен научно-методический аппарат применения робототехнических комплексов военного назначения (РТК ВН) в Вооруженных Силах РФ: обоснование задач и оценка эффективности; структурная модель решения ситуационной задачи; методологические основы теории и практики. Определен подход к формированию форм и способов их применения.

КЛЮЧЕВЫЕ СЛОВА

РТК ВН, модель решения задачи, классификация задач, боевые задачи, обеспечивающие задачи, формы и способы применения РТК ВН.

ABSTRACT

The paper presents a research and methodology apparatus of using military-purpose robotechnical systems (MP RTS) in the RF Armed Forces, namely, justification of the tasks and assessment of the effectiveness, the structural model of situational problem solution, the methodological basis of the theory and practice. It also maps out the approach to outlining the forms and methods of their employment.

KEYWORDS

MP RTS, problem solution model, task classification, combat assignments, supporting tasks, forms and methods of using MP RTS.

ОДНИМ из приоритетных направлений совершенствования отечественного оружия является развитие систем и комплексов вооружения, военной и специальной техники (ВВСТ) на основе технологий робототехники и интеллектуальных процессов управления.

Под РТК ВН понимаются дистанционно управляемые или автономные образцы ВВСТ, в том числе беспилотные летательные аппараты (БПЛА), предназначенные для выполнения боевых и обеспечивающих задач без полного или частичного участия в них человека[1].

Обычно при определении потребности в РТК ВН выделяют три основных преимущества, которые позволяют внедрить их в войска[2-5]:

первое — уменьшение потерь личного состава и техники при выполнении боевых и других рискованных задач;

второе — повышение эффективности решения как известных, так и появившихся новых задач, недоступных для решения человеком вследствие физиологических и интеллектуальных ограничений;

третье — минимизация численности личного состава, необходимого для обеспечения решения существующих задач.

Целями применения РТК ВН являются[6],[7]:

- повышение эффективности боевого применения частей и подразделений;
- снижение риска и минимизация боевых (санитарных и безвозвратных) потерь личного состава в различных условиях подготовки и ведения боевых действий с применением различных видов оружия;
- выполнение сложных монотонных действий и опасных операций в труднодоступных местах, а также в условиях техногенных катастроф, чрезвычайных ситуаций (ЧС) и аварий.

Для формирования научно-обоснованного замысла применения РТК ВН в войсках на долгосрочный период считаем необходимым выполнение комплексных научных исследований по разработке методического аппарата обоснования перечня решаемых войсками задач, для которых необходимо и оправдано их применение. Эти задачи должны оцениваться количественными характеристиками, иллюстрирующими преимущества применения РТК ВН в сравнении с обычным вооружением. Такими характеристиками могут быть численные показатели, отражающие, например, прогнозируемые потери военнослужащих, предельно допустимые значения психофизиологических нагрузок, опасный уровень радиационной зараженности местности и др.

Разработка методического аппарата обоснования перечня задач, для решения которых необходимо и целесообразно применение РТК ВН, создание комплексных моделей и методик оценки их эффективности должны реализовываться как комплекс взаимоувязанных исследований.

Предлагаемая структура данных исследований (научно-методического аппарата) представлена на рисунке 1. Его основу составляют аналитические и имитационные модели для обследования среды содержания и профессиональной жизнедеятельности военнослужащих в условиях критического уровня потенциальных угроз. Результатами исследований с применением указанных моделей могут быть, например, методики идентификации опасностей, методики оценки рисков потерь, травматизма, профзаболеваний и других негативных исходов, связанных с профессиональной деятельностью военнослужащих[8,9].

Ниже в статье раскрыты и представлены структурные элементы научно-методического аппарата, исходным из которых является ***определение перечня задач соединениям, частям и подразделениям, решаемым с применением различных типов РТК ВН***. Проведенный анализ вариантов целевого предназначения РТК ВН показал, что для них среди возможных можно выделить три группы задач: ***боевые*** (физическое или огневое воздействие на противника), ***обеспечивающие и учебно-боевые***[10,11,12].

Существующие в настоящее время в Вооруженных Силах РФ РТК ВН являются средствами решения определенного круга боевых и обеспечивающих задач. Они могут применяться для контроля обстановки, уничтожения живой силы, военной техники и объектов противника, наблюдения за маршрутами движения, ведения разведки, наведения сил и средств быстрого реагирования на диверсионно-разведывательные группы, террористические группы и т. д. Именно

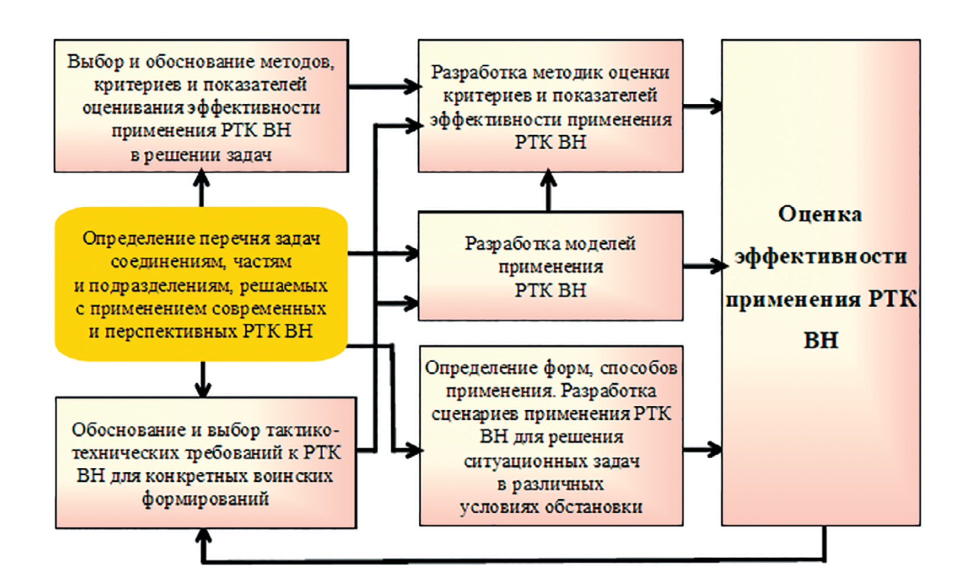


Рис. 1. Научно-методический аппарат обоснования задач и оценки эффективности применения РТК ВН

они могут стать основным элементом формирования единого информационного поля в районах расположения частей и соединений.

В связи со спецификой задач, решаемых частями и подразделениями, например, Ракетных войск стратегического назначения или Воздушно-космических сил, наиболее актуальным применением РТК ВН в настоящее время является решение обеспечивающих задач. Поэтому рассмотрим основные направления применения РТК ВН при их решении. Анализ исследований[13,14,15] показал, что такими направлениями могут быть ***боевое, техническое, тыловое и морально-психологическое обеспечения.***

Перспективными направлениями применения РТК ВН могут быть: решение разведывательно-ударных задач при ведении борьбы с диверсионно-разведывательными формированиями противника в районах расположения частей и подразделений; ретрансляция сигналов в различных радиосетях; доставка грузов и т. д.

Анализ условий решения обеспечивающих задач показал, что практически все они могут выполняться с применением РТК ВН, за исключением доставки личного состава очередных смен при смене с боевого дежурства[16,17,18]. Был проведен также анализ авиационного обеспечения, решаемого в частях и подразделениях применением вертолетов и возможной их заменой на РТК ВН[19,20].

Результаты анализа показали, что применение РТК ВН в сравнении с пилотируемыми системами имеет ряд преимуществ, основными из которых являются:

- стоимостные и эксплуатационные затраты РТК ВН в значительной степени ниже пилотируемых;
- тактико-технические и летные характеристики РТК ВН превосходят пилотируемые;
- боевое применение не сопряжено с риском потери экипажа;
- применение отдельных классов РТК ВН не требует взлетно-посадочной полосы;
- отсутствие сезонных и географических ограничений к применению, мобильность;

• относительная простота по конструкции и надежность в эксплуатации;

• низкая стоимость летного часа, вытекающая из сравнительно низкой стоимости самого аппарата и малого расхода топлива (1 час эксплуатации БПЛА — 20—50 долл., вертолета — 2000—2500 долл.)[21];

• низкие требования к подготовке наземного обслуживающего персонала.

Принципиально новым качественным показателем разведки с применением воздушных РТК ВН является длительность патрулирования в воздушном пространстве и минимальная заметность, что позволяет вести длительное скрытое наблюдение.

В частности, боевое обеспечение осуществляется при решении разведывательно-ударных задач ведения борьбы с диверсионно-разведывательными формированиями противника в районах расположения частей и подразделений, ретрансляции сигналов в различных радиосетях, доставки различных грузов и т. д.

Таким образом, результаты проведенных исследований[22,23,24] показали возможность решения в войсках значительного количества задач всестороннего обеспечения, при этом больше половины из них — в рамках различных видов боевого обеспечения. В РВСН в настоящее время воздушные РТК ВН применяются при решении задач разведки, охранения, маскировки.

Отметим, что задач, потенциально решаемых с применением перспективных РТК ВН, значительно больше. Проведенными исследованиями определено их более двадцати. На рисунке 2 представлена структурная модель решения каждой из них. Она разработана на основе анализа возможного применения РТК ВН в боевых условиях, в условиях выполнения

В связи со спецификой задач, решаемых частями и подразделениями, например, Ракетных войск стратегического назначения или Воздушно-космических сил, наиболее актуальным в настоящее время для применения РТК ВН является их всестороннее обеспечение. Анализ исследований показал, что направлениями обеспечения могут быть боевое, техническое, тыловое и морально-психологическое.

обеспечивающих и учебно-боевых задач и состоит из трех основных блоков. Блоки предназначены: входной — для ввода исходных данных; оператор — для проведения промежуточных расчетов; выходной — для получения окончательного результата, оценки эффективности решения конкретной задачи, формирования отчетных материалов.

Важным элементом научно-методического аппарата является ***обоснование и выбор тактико-технических требований к РТК ВН*** исходя из особенностей подготовки и ведения боевых действий частями и соединениями различных видов и родов войск, их расположения в районах дислокации (позиционных районах) и решения поставленных задач. Эти требования подразделяются на общие и частные.

Общие — определяют правила функционирования РТК ВН, обеспечивающие деятельность воинских частей и подразделений, основными из которых являются:

• высокая эффективность функционирования при решении задач в любых условиях обстановки;

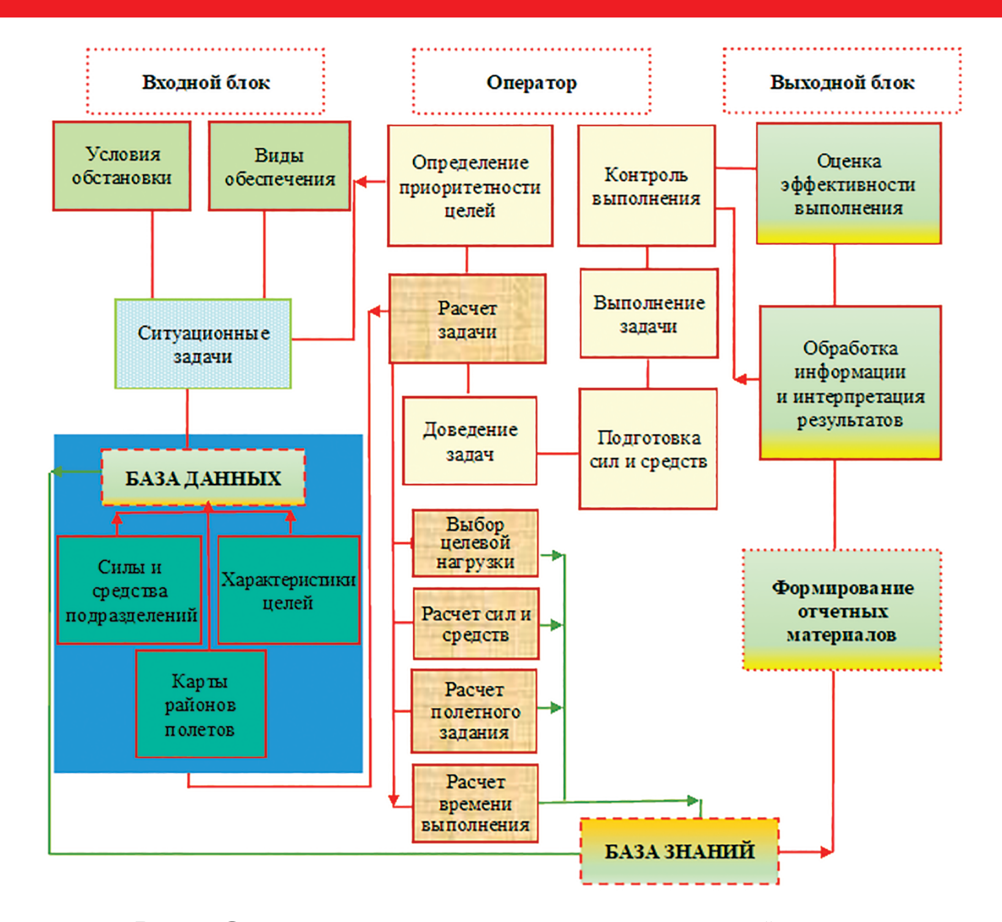


Рис. 2. Структурная модель решения ситуационной задачи

• работоспособность в условиях огневого, радиоэлектронного и информационного воздействия противника по объектам частей и соединений, а также при радиационном, химическом или биологическом заражениях местности;

• действия нескольких разноплановых РТК ВН в составе групп, ретрансляция команд управления между отдельными РТК;

• дистанционное управление целевой нагрузкой управляемых РТК ВН в режиме реального времени;

• непрерывный контроль соответствия режимов движения управляемых РТК ВН;

• унифицированные, помехозащищенные каналы управления и связи (каналы управления и передачи данных);

• регистрация всех информационных потоков, поступающих в РТК ВН, их перегрузка на внешний носитель информации;

• автоматизированный сбор, обработка и обобщение данных (формализованных приказов, команд), циркулирующих РТК ВН, их получение и анализ оператором;

• невозможность воздействия РТК ВН по боевым порядкам своих войск и другие.

Частные — исходя из специфики деятельности соединений и частей видов и родов войск, особенностей решаемых задач, включают требования к конкретному составу комплекса, его бортовому и наземному оборудованию, целевой нагрузке и т. д.

Широкое применение РТК ВН в войсках привело к необходимости

поиска и обоснования форм и способов их применения. Под применением ВВСТ принято понимать использование, употребление их для решения определенных задач[25]. Систематизация теоретических фундаментальных основ отечественной военной науки, проведенный ретроспективный анализ терминов и определений сущности и содержания форм и способов применения ВВСТ, выводов и результатов научно-исследовательских работ по данной тематике[26-30] позволили сформировать для тактического уровня следующий методический подход к определению содержания и выбору форм и способов применения РТК ВН.

Поскольку любой способ выражает собой содержание действий, а его, в свою очередь, составляют решаемые задачи, то в дальнейшем при определении способов необходимо учитывать перечень задач, решаемых с применением РТК ВН.

При определении, разграничении способов применения РТК ВН следует исходить прежде всего из конкретной цели, выдвигаемой лицом, уполномоченным принимать решение на их применение в соответствии с условиями боевой обстановки на данный момент и ближайшую перспективу их развития. Кроме того, необходимыми признаками (существенными критериями) определения и отличия одного способа от другого должны являться пространственно-временное и количественное распределение применяемых РТК ВН, характеризующее боевой порядок и специфику взаимодействия его элементов для выполнения назначенных им задач.

Предложенный подход позволяет предложить вариант типологии (классификатора) способов применения РТК ВН для различных классификационных признаков.

1. По решаемым задачам: а) боевое, б) ***обеспечивающее***, в) учебно-боевое.

2. По отношению к началу воздействия противника: а) ***упреждающее***, б) ответное, в) ответно-встречное.

3. По плановости применения: а) ***плановое***, б) внеплановое, в) в распорядительном порядке.

4. По порядку применения: а) последовательное, б) ***одновременное (параллельное)***, в) комбинированное.

5. По интенсивности применения: а) ***однократное (разовое)***, б) регулярное (систематическое).

6. По количеству привлекаемых средств (РТК ВН): а) одиночное, б) ***групповое,*** в) массированное.

7. По видам среды применения РТК ВН: а) воздушное, б) ***наземное***.

8. По характеру воздействия на силы и средства противника: а) ***пассивного действия***, б) активного действия.

9. По характеру передачи добытой и управляющей информации (доведения, обмена): а) в режиме реального времени, когда информация передается постоянно дистанционно, в режиме реального времени и решение по ней принимается командиром (оператором) немедленно; б) ***дискретно*** (периодически, в назначенное время, по запросу, по факту поступления критериально значимых данных), через определенные промежутки времени, по мере накопления и обработки, поступления, доставки информации (дистанционно или после прибытия РТК ВН в исходный пункт и дешифровки доставленной информации).

В итоге соответствующее развернутое описание данного способа применения РТК ВН с помощью предложенного классификатора с «композицией» признаков (отмечены ***курсивом)*** может иметь примерно следующий вид: *обеспечивающее упреждающее плановое одновременное однократное применение группы наземных РТК ВН пассивного действия с дискретной передачей информации*

(информационным обменом). Очевидно, что такой способ характерен для решения различного типа разведывательных задач. При этом для решения каждой из них для каждого РТК ВН (группы РТК ВН) будут использоваться традиционные (известные) способы их решения, характерные для решения задач существующих видов обеспечения и возможностей применяемых РТК ВН.

Использование разработанной систематизации (типологии, классификатора) классификационных признаков открывает возможности:

во-первых, достаточно полной характеризации (определения, описания) любого способа применения РТК ВН (даже потенциально возможного) посредством формирования композиции (выборки, совокупности) признаков, обеспечивающих однозначную идентификацию конкретного способа;

во-вторых, математического моделирования и оценивания (прогнозирования) эффективности применения любого способа (для заданных условий обстановки, допущений и ограничений);

в-третьих, оптимизации планирования и управления его практической реализацией.

Немаловажными преимуществами данной системы признаков являются ее открытый характер, допускающий дополнение и корректировку, развитие, универсальность использования в перспективе.

Таким образом, предложенная классификация может рассматриваться в качестве исходной для формирования перечня основных способов возможного применения РТК ВН в различных видах и родах войск Вооруженных Сил РФ.

При выборе форм применения РТК ВН будем исходить из того, что под формой военных (боевых) действий принято понимать внешнее

Предложенный подход к описанию способов применения РТК ВН с помощью предложенного классификатора признаков может рассматриваться в качестве исходного для различных видов и родов Вооруженных Сил Российской Федерации.

выражение, организационную сторону действий, взаимоувязывающую цель, задачи, масштабы действий, состав привлекаемых войск, специфику управления ими, другие признаки и условия действий[31]. Форма, отражая организационную сторону боевых действий, их масштаб, а также характер используемого оружия, тесно связана со способом, характеризующим порядок и приемы применения сил и средств (вооружений и техники) для решения поставленных задач.

В соответствии с изложенным, сопоставляя и интегрируя обозначенные способы с существенными признаками и условиями осуществления форм действий подразделений РТК ВН в интересах видов и родов войск, представляется рациональным различать и необходимым рассматривать в дальнейшем три основные формы применения РТК ВН: **боевое, обеспечивающее и учебно-боевое**. Прежде всего следует четко определиться с этими понятиями.

Под **боевым применением** РТК ВН следует понимать систему мероприятий, проводимых в ходе ведения боевых действий и заключающихся в активном целенаправленном воздействии физическими факторами (в том числе огнем, радиоэлектронным или лазерным импульсом, инфра- и ультразвуковыми волнами

В интересах видов и родов войск Вооруженных Сил Российской Федерации наиболее рациональными и необходимыми основными формами применения РТК ВН целесообразно в дальнейшем рассматривать: боевое, обеспечивающее и учебно-боевое.

и т. п.) на боевые формирования и вооружение (средства) противника в целях активного противодействия деятельности противника, поражения его живой силы (уничтожение, подавление, вывод из строя), боевых и технических средств, нарушения управления (уничтожение, вывод из строя пунктов управления и связи), создания условий, при которых устойчивое функционирование и выполнение задач затруднено, ограничено или невозможно.

В свою очередь, определенная выше классификация задач, которые наиболее вероятно могут быть возложены на РТК ВН, позволяет сформулировать определение второй основной формы применения РТК ВН.

Обеспечивающее применение — комплекс мероприятий, проводимых с применением РТК ВН при подготовке и ведении боевых действий, который направлен на:

• информационное обеспечение командиров и штабов данными о противнике, состоянии своих войск и обстановке в районах расположения;

• снижение потерь личного состава, вооружения, средств боевого управления и связи, техники, материальных средств различного назначения;

• наиболее полное использование боевых и эксплуатационных свойств ракетных комплексов;

• выполнение задач в неблагоприятных условиях обстановки;

• восстановление боеспособности в случае ее нарушения.

По аналогии с предыдущими дадим понятие **дефиниции учебно-боевого применения** как комплекса мероприятий боевой подготовки, выполняемых в целях обучения, совершенствования и контроля навыков и умений личного состава (практического выполнения действий на тренажерах и учебно-боевых образцах робототехники) по развертыванию (приведению в готовность к применению), эксплуатации, работе с агрегатами и системами РТК ВН при выполнении задач, организации управления и взаимодействия, в том числе с проведением стрельб на учебном полигоне (тактическом поле) и т. п. Как особую разновидность этой формы с определенными оговорками и допущениями можно рассматривать комплекс мероприятий по приемо-сдаточным производственным и полигонным государственным испытаниям вновь разработанных образцов РТК ВН.

Разработанные подходы к определению перечня задач, вариантов способов и форм применения РТК ВН применительно к специфике тактики соединений и частей видов и родов войск Вооруженных Сил РФ, особенностям их боевого применения не являются исчерпывающими и носят характер предварительных, начальных ориентиров. В дальнейших исследованиях этого вопроса они могут и должны быть скорректированы и дополнены по мере принятия и реализации концептуальных, программных и этапных решений по разработке, испытаниям и принятию конкретных образцов РТК ВН на вооружение, а также с учетом накопления частями и соединениями как боевого, так и учебно-боевого опыта их применения.

Эффективность РТК ВН в общем виде определяется факторами, характеризующими, во-первых, качество и состояние его готовности к применению, во-вторых, уровень обученности и компетентности специалистов, в-третьих, качество управления и всестороннего обеспечения РТК ВН.

Конечным элементом научно-методического аппарата является определение ***эффективности применения РТК ВН***. Эффективность РТК ВН, как любого технического средства вооруженной борьбы, в общем виде определяется посредством трех групп основных факторов, характеризующих[32,33,34]:

• качество РТК ВН с включением уровня тактико-технических, эксплуатационных характеристик и состояния готовности к применению по предназначению;

• уровень подготовки (профессиональной компетентности и обученности) специалистов РТК ВН;

• качество управления применением РТК ВН, в том числе организации обеспечения применения.

Перечисленные факторы характеризуют РТК ВН с точки зрения его функциональных возможностей, квалификации обслуживающего персонала, качества управления его применением.

На основе анализа результатов оценки эффективности РТК ВН можно определить степень влияния тактико-технических характеристик (ТТХ) и способов их применения на эффективность боевых действий для использования в дальнейшем в двух направлениях:

первое — для синтеза и обоснования рациональных вариантов применения уже существующих РТК ВН в интересах повышения качества управления в целях более полной реализации их потенциальных боевых возможностей;

второе — для обоснования тактико-технических требований к создаваемым РТК ВН и определения облика перспективных образцов.

Для оценки эффективности применения РТК ВН целесообразно использовать следующие группы критериев и показателей[35,36]: *боевые* (боевой потенциал, предотвращенные потери ВВСТ и личного состава, нанесенный противнику ущерб, оперативность решения задач); *целевые* (вероятность и качество выполнения задач); *эксплуатационные* (надежность, ремонтопригодность, унификация и т. п.) и *экономические*.

Таким образом, подводя итог изложенному выше, можно сделать следующие выводы. Части и подразделения при активном применении современных и перспективных РТК ВН имеют достаточно возможностей для своевременного и качественного решения стоящих перед ними задач. Это, в свою очередь, позволит:

• повысить эффективность боевого применения войск;

• снизить риск и минимизировать боевые потери личного состава в различных условиях подготовки и ведения войны с применением различных средств поражения;

• выполнить сложные монотонные действия и опасные операции в труднодоступных местах, а также в условиях техногенных катастроф, ЧС и аварий, пожаров.

Исходя из полученных выше результатов, разработанный научно-методический аппарат целесообразно применить для определения эффективности решения отдельных задач технического, тылового, меди-

цинского и морально-психологического обеспечения боевых действий соединений, частей и подразделений видов и родов войск Вооруженных Сил Российской Федерации с применением РТК ВН.

ПРИМЕЧАНИЯ

[1] *Гладышев А.И., Зайцев А.В., Куканков С.Н.* Робототехнические комплексы военного назначения. Балашиха: ВА РВСН им. Петра Великого, 2016. 197 с.

[2] Там же.

[3] *Хачатрян А.В., Ветрюк М.С.* Сравнительная оценка характеристик, принятых на вооружение и перспективных образцов робототехнических комплексов военного назначения в соединениях и частях РВСН / Сборник научных трудов «Труды 4 ЦНИИ МО РФ». Королев, 2020.

[4] *Хачатрян А.В.* Особенности применения БпЛА в интересах решения задач воинских подразделений и формирований / Материалы XXIV Международной НПК №47/4. Химки: АГЗ МЧС России, 2014.

[5] *Хачатрян А.В.* Методический подход к классификации задач, решаемых с применением БпЛА в ходе вооруженных конфликтов / Сборник трудов IV Всероссийской НТК 4 ЦНИИ МО РФ. Королев, 2020.

[6] *Хачатрян А.В., Ветрюк М.С.* Сравнительная оценка характеристик…

[7] *Хачатрян А.В.* Особенности применения БпЛА…

[8] Там же.

[9] *Хачатрян А.В.* Методический подход к классификации задач…

[10] Там же.

[11] *Хачатрян А.В.* Особенности применения БпЛА…

[12] *Селезнев М.Е., Федотов С.А., Новиков Д.В.* О применении робототехнических комплексов военного назначения // Проблемы эффективности и безопасности функционирования сложных технических и информационных систем / Труды XXXVII Всероссийской НТК. Серпухов, филиал ВА РВСН, 2018.

[13] Там же.

[14] *Хачатрян А.В.* Особенности применения БпЛА…

[15] *Хачатрян А.В.* Методический подход к классификации задач…

[16] Там же.

[17] *Селезнев М.Е., Федотов С.А., Новиков Д.В.* О применении робототехнических комплексов…

[18] *Хачатрян А.В.* Особенности применения БпЛА…

[19] Там же.

[20] *Хачатрян А.В.* Методический подход к классификации задач…

[21] *Гладышев А.И., Зайцев А.В., Куканков С.Н.* Робототехнические комплексы военного назначения.

[22] *Хачатрян А.В., Ветрюк М.С.* Сравнительная оценка характеристик

[23] *Хачатрян А.В.* Особенности применения БпЛА…

[24] *Хачатрян А.В.* Методический подход к классификации задач…

[25] Энциклопедия РВСН. М., 2014. 874 с.

[26] *Хачатрян А.В., Ветрюк М.С.* Сравнительная оценка характеристик…

[27] *Селезнев М.Е., Федотов С.А., Новиков Д.В.* О применении робототехнических комплексов…

[28] *Хачатрян А.В.* Особенности применения БпЛА…

[29] *Хачатрян А.В.* Методический подход к классификации задач…

[30] *Гладышев А.И., Зайцев А.В., Куканков С.Н.* Робототехнические комплексы военного назначения.

[31] Энциклопедия РВСН. М., 2014. 874 с.

[32] *Хачатрян А.В.* Особенности применения БпЛА…

[33] *Хачатрян А.В.* Методический подход к классификации задач…

[34] *Гладышев А.И., Зайцев А.В., Куканков С.Н.* Робототехнические комплексы военного назначения.

[35] Там же.

[36] *Хачатрян А.В., Ветрюк М.С.* Сравнительная оценка характеристик…

Прогностическая оценка тенденций развития средств вооруженной борьбы и способов их применения в войнах будущего

Подполковник запаса А.С. УЛАНОВ,
кандидат технических наук

АННОТАЦИЯ

Рассматриваются возможные причины будущих войн и цели участвующих в них государств. На основе анализа перспектив научно-технического прогресса спрогнозированы некоторые ожидаемые тенденции развития средств вооруженной борьбы и способов их применения в возможных военных конфликтах в середине и последней трети XXI века.

ABSTRACT

The paper looks at likely causes of would-be wars and the objectives of participant states. It falls back on the analysis of science-and-technology progress to forecast some expected development trends for armed struggle assets and methods of their employment in potential military conflicts in the middle and last third of the 21st century.

КЛЮЧЕВЫЕ СЛОВА

Средства вооруженной борьбы, искусственный интеллект, псевдокосмические аппараты, атрибутивный БПЛА, безэкипажный корабль, кибероружие.

KEYWORDS

Armed struggle assets, artificial intelligence, pseudo-space vehicles, attributive UAV, crewless ship, cyber weapons.

СОВРЕМЕННОЕ поколение людей живет в условиях необычайно динамично меняющего мира. Изменения успевают затронуть все сферы человеческой деятельности и общественных отношений на протяжении жизни всего одного поколения, что не имело прецедентов в предыдущих исторических периодах[1]. Не составляет исключения и военное дело, где происходят как минимум не менее динамичные преобразования, обусловленные прежде всего научно-техническим прогрессом, который и определяет основные направления развития средств вооруженной борьбы и способов их применения в современных и будущих военных конфликтах.

Причины будущих войн и цели участвующих в них государств

Способы ведения войн и их характер предопределяются целями участвующих в них государств и возможностями имеющихся в их распоряжении средств вооруженной борьбы. В связи с этим представляется целесообразным рассмотреть, какие цели могут преследовать государства в будущих войнах и какие технологии создания вооружения, военной и специальной техники (ВВСТ) могут стать им доступны в XXI веке.

Провоцировать военные конфликты между государствами в XXI веке могут, на наш взгляд, следующие основные факторы[2,3,4]**:**

- глобальные изменения климата;
- рост количества и плотности населения, приводящий к всемирному и региональному дефициту пищевых, водных и энергетических ресурсов;
- ухудшение в отдельных регионах экологической обстановки;
- истощение мировых или региональных запасов углеводородного топлива и неравномерность распределения по планете известных в настоящее время альтернативных энергетических ресурсов;
- исчерпание возможностей существующей общественно-экономической модели развития, переход на новую форму международных экономических и политических отношений (цифровая цивилизация и трансгуманизм).

Следует также учитывать тот факт, что, несмотря на переход мировой цивилизации в постиндустриальную эпоху, когда большое значение приобрели нематериальные ценности, которые не имеют принадлежности к территории и которые невозможно «отобрать силой» (например, информационные технологии), человечество по-прежнему нуждается в энергии, продовольствии и материальных благах.

Цели войны подразделяются на политические и стратегические. Первые — это макрорезультаты, которые рассчитывают получить правящие элиты государства-агрессора при победе в войне, т. е. то, ради чего данное государство вступает в войну. Определяются они на основе общей концепции, доктрины и направленности развития государства, которые, в свою очередь, формируются исходя из трендов эволюции внутренних экономических, политических и общественных взаимоотношений.

Стратегические цели — это непосредственно глобальные военные задачи (цели военной кампании, стратегической военной операции и т. п.), которые необходимо решить, чтобы достичь победы.

С учетом изложенного **нападающее государство может, на наш взгляд, ставить в войнах будущего следующие истинные** (а не публично декларируемые или закамуфлированные) **политические цели**:

- обеспечение доступа к энергоресурсам, рудным и нерудным полезным ископаемым, сельскохозяйственным ресурсам, биоресурсам и источникам пресной воды, а также к территориям с комфортными для проживания климатическими условиями и благополучной экологической обстановкой;
- ослабление или полное уничтожение государств, выступающих глобальными экономическими конкурентами для агрессора, либо получение контроля над деятельностью их органов власти.

Следует иметь в виду, что политическая и военная конкуренция между государствами является лишь средством достижения их интересов в экономической сфере. Межнациональные (этнические) и межконфессиональные противоречия в качестве факторов, способствующих возникновению войн, равно как и постановка политической цели войны в интересах разрешения данных противоречий, в настоящей статье не рассматриваются, так как автор полагает их вторичными по отношению к ранее приведенным факторам и целям.

Рассмотрим **возможные методы достижения целей войн будущего**. Обеспечить доступ к природным ресурсам и территориям можно, во-первых, путем получения достаточного (для реализации замыслов) административного контроля над территориями противника, а во-вторых, посред-

ством принуждения органов власти государства-жертвы к предоставлению победителю доступа к интересующим ресурсам и территориям на желаемых для него условиях.

В первом случае нападающей стороне придется установить военный контроль над оспариваемой территорией. Во втором — достаточно принудить действующие органы власти атакуемого государства к требуемым политическим и законодательным решениями, либо установить в нем лояльный правящий режим. Оба результата могут быть достигнуты как военными, так и невоенными средствами, а также их сочетанием. Но в данной статье рассмотрим только военные средства достижения политических целей.

Чтобы установить военный контроль над оспариваемой территорией, нападающей стороне необходимо нанести поражение вооруженным силам (ВС) противника, обеспечив при этом защиту собственной территории, населения, объектов инфраструктуры и экономического комплекса от ответных ударов, сместить политическое руководство государства, а также создать для его жителей «фактор страха», не позволяющий оказывать организованное сопротивление.

В качестве «фактора страха» могут выступать угрозы физического уничтожения части населения, нанесения неприемлемого экологического ущерба территории, полного или частичного уничтожения инфраструктуры (в первую очередь объектов транспортной сети, энергообеспечения, водоснабжения) и критических элементов экономического комплекса. Причем реализовать данный фактор необходимо так, чтобы не навредить поставленным политическим целям, т. е. не нарушить в интересующих аспектах экологическую ситуацию, не вывести из строя те объекты инфраструктуры, которые представляют интерес для дальнейшего использования и т. п. Таким образом, действия по обеспечению убедительности угрозы не должны перейти некий разумный рубеж вмешательства.

Для принуждения органов власти государства-жертвы к решениям, которые требует от них нападающая сторона, достаточно лишить его ВС способности к ответному удару и обеспечить вышеупомянутый «фактор страха». В дальнейшем военно-политических лидеров государства-жертвы могут заставить передать власть лояльным к агрессору политикам с созданием марионеточного правительства, т. е. фактически должна произойти смена политического режима.

Если же политической целью войны является ослабление либо уничтожение государства-конкурента, то необходимо сокрушить его военный потенциал, лишив ВС противника возможности нанесения ответных ударов, частично или полностью вывести из строя объекты государственного и военного управления, оборонно-промышленного и топливно-энергетического комплексов страны, транспортной инфраструктуры, коммунального хозяйства и др. Данные меры могут сочетаться с физическим уничтожением политических и военных лидеров противника.

Следует учитывать тот факт, что, несмотря на переход мировой цивилизации в постиндустриальную эпоху, когда большое значение приобрели нематериальные ценности, которые не имеют принадлежности к территории и которые невозможно «отобрать силой» (например, информационные технологии), человечество по-прежнему нуждается в энергии, продовольствии и материальных благах.

Развитие средств вооруженной борьбы и способов их применения в середине XXI века

Определяющее влияние на облик ВВСТ и способы их применения в войнах будущего окажет развитие техники и технологий. Ведущие мировые ученые-футурологи в области прогнозирования эволюции прикладной науки полагают, что к середине XXI века значительный прогресс произойдет в развитии робототехники, технологий искусственного интеллекта (ИИ) и экспертных систем, а также сетевых информационных технологий[5,6]. А к концу текущего столетия следует ожидать прорывных достижений в области био- и нанотехнологий, а также программируемой материи.

В последней трети XXI века совокупность перечисленных технологий позволит создавать самовосстанавливающиеся (саморегенерируемые) образцы ВВСТ, а также самоперестраиваемые модульные робототехнические комплексы (РТК), внутренняя структура и строение которых адаптируются к выполняемой задаче.

С учетом данных тенденций развития техники и технологий основной особенностью военных конфликтов середины XXI века станет их сетецентричность. При этом нападающая сторона для достижения своих политических целей будет стремиться сохранить экологическую среду оспариваемого пространства, а также интересующие ее объекты инфраструктуры. Поэтому наиболее вероятным способом военных (боевых) действий станет нанесение прицельных точечных ударов без широкого применения «ковровых» бомбометаний и традиционного оружия массового поражения (ОМП).

Следует ожидать, что **вооруженное противоборство в рассматриваемый период будет, на наш взгляд, развиваться по следующим основным направлениям**:

- продолжение милитаризации околоземного космического пространства, размещение в нем ударных вооружений;
- роботизация ВВСТ, появление высокоавтономных боевых систем во всех сферах вооруженной борьбы, переход от управления отдельными тактическими единицами (образцами ВВСТ) и тактическими группам к системам управления на основе ИИ;
- существенное увеличение срока автономности беспилотных (безэкипажных) ударных средств, размещаемых в воздушно-космической и водной (надводной и подводной) физических средах;
- широкое распространение гиперзвукового оружия в воздушной среде и сверхзвукового — в водной;
- значительное снижение радиоакустической (электромагнитной и акустической) заметности большинства образцов наступательных вооружений;
- дальнейшее развитие и совершенствование технологий информационных и психологических операций;
- развитие кибернетического оружия и активное противоборство в киберпространстве;
- вывод военнослужащих (боевых расчетов) за пределы зоны воздействия оперативного и тактического оружия противника, высвобождение их от участия в огневом контакте;
- отстранение военнослужащих от управления ВВСТ в бою, исключение их из процесса «разведка—целеуказание—поражение». Их деятельность, вероятно, ограничится лишь планированием боевых действий, постановкой задач тактическим и оперативным единицам, координацией и контролем результатов боевых действий.

Прогнозируется, что основной движущей силой развития ВВСТ

и способов их применения уже в середине XXI века станут технологии ИИ. Произойдет переход от автоматизации к интеллектуализации, т. е. внедрению высокоинтеллектуальных средств вооруженной борьбы. Уже сейчас США в своей Инновационной оборонной инициативе (*DII*) объявили о переходе к ***Третьей стратегии компенсации*** (*СК-3*), призванной обеспечить их военное доминирование в мире путем широкомасштабного использования ИИ в системах вооружений.

Внедрение ИИ в сферу вооруженной борьбы оценивается экспертами министерства обороны США таким же образом, как изобретение пороха и ядерного оружия, т. е. как фактор, способный полностью изменить саму парадигму военных действий. Ожидается, что применение ИИ позволит разорвать связь между численностью населения и возможностями экономики государства, с одной стороны, и боеспособностью ВС — с другой. По мнению американских системных аналитиков, в ситуации, когда противоборствующие стороны имеют ударные вооружения, дающие возможность несколько раз полностью уничтожить противника, соревноваться дальше в их совершенствовании не имеет смысла.

Соперничество перейдет в плоскость систем управления — ИИ против ИИ. В случае когда одна сторона посчитает, что ее ИИ мощнее, она может решиться на нанесение удара. Если в настоящее время ведущие державы ведут диалог по вопросам ограничения ядерных и ракетных вооружений, ОМП и систем противоракетной обороны (ПРО), то в скором времени вполне может встать вопрос о заключении соглашений по ограничению применения технологий ИИ в военных целях.

Основное вооруженное противоборство, определяющее общий исход войны, в рассматриваемый период будет, на наш взгляд, проходить в воздушно-космической сфере. Главными целями ударов воздушно-космических сил станут не группировки войск противника на театре военных действий (ТВД), а объекты его инфраструктуры и стратегический тыл даже у государств с большой территорией. Высокоточное дальнобойное неядерное оружие сможет через воздушно-космическую среду воздействовать на объекты противника на любом удалении. Ареной военных действий станет вся планета: поверхность суши, ее океанские и морские акватории, воздушно-космическое пространство.

Содержание таких фундаментальных категорий современной теории военного искусства, как стратегическое развертывание, стратегическое наступление или стратегическая оборона группы фронтов, стратегическая перегруппировка войск, стратегический маневр, стратегические резервы и другие утратит смысл. Стратегия и оперативное искусство станут трудноразделимы.

Уровень развития ВВСТ и военного искусства во многих случаях позволит полностью достигать целей войны через воздушно-космическую сферу, без перехода к полноценным морским и наземным боевым действиям. В космическом пространстве нет ограничений по количеству и объему развертываемых ударных средств. Действительное назначение космического оружия определить трудно. Оно может быть замаскировано под другие сугубо гражданские системы, т. е. никаких политических препятствий для его развертывания сейчас не существует. Применение живой силы и наземных группировок войск станут в войнах будущего не потенциальным преимуществом, а большим недостатком.

Воздушное и космическое пространство, вероятно, станут единой

сферой вооруженной борьбы, что обусловлено рядом значимых факторов.

Во-первых, группировка космических аппаратов (КА) начнет выполнять не только обеспечивающие функции (разведка, связь, навигация, картографирование, метеообеспечение, радиоэлектронная борьба (РЭБ) и т. п.), но и ударные. По сути, космические ударные вооружения, содержащиеся в высокой степени готовности к боевому применению, будут представлять собой стратегические неядерные силы, вынесенные за пределы собственной территории и предназначенные как для нанесения ударов по объектам на поверхности Земли, так и для борьбы с КА противника.

Во-вторых, широкое распространение получат беспилотные средства воздушно-космического нападения, способные действовать и в воздушном, и в космическом пространстве, совершая многократные маневры по высоте.

В-третьих, с высокой вероятностью в середине XXI века ряд государств развернет ПРО космического базирования.

Как следствие, в ближней космической зоне развернется полноценное огневое противоборство. Военные действия, скорее всего, будут начинаться из космоса или в том числе из космоса. При радиоэлектронном подавлении или потере в ходе боевых действий части обеспечивающих КА их функции частично смогут взять на себя псевдокосмические аппараты (высотные беспилотные летательные аппараты (БПЛА) сверхдлительного барражирования или воздухоплавательные платформы).

Первоочередными объектами поражения космическими боевыми ударными системами в будущей войне могут стать стационарные центры государственного и военного управления и связи; аэродромы и ракетные комплексы ответного удара; системы энергоснабжения; предприятия военно-промышленного и топливно-энергетического комплексов; центры по переработке ядерного сырья и производству ОМП.

Основу средств воздушного нападения составят БПЛА, обладающие высокой функциональной автономностью. За пилотируемыми платформами останутся функции воздушных командных пунктов, действующих вне зоны воздействия тактических огневых средств противника (для воздушных командных пунктов высших звеньев управления — вне зоны досягаемости оперативного оружия). Остальные задачи военной авиации — нанесение ударов, разведка, наблюдение, РЭБ, обеспечение связи в оспариваемом пространстве, отвлекающие (демонстративные) действия — будут возложены в основном на БПЛА, объединенные в многоуровневые технические экосистемы. Тяжелые БПЛА, применяющие ударное высокоточное оружие (ВТО) дальнего действия, станут также носителями и/или координаторами более легких и дешевых специализированных БПЛА малого класса, которые смогут выполнять другие задачи (разведка, связь, РЭБ, нанесение ударов). Поскольку последние достаточно дешевы, потеря части из них будет приемлемой по критерию стоимости.

Так, уже в настоящее время в ряде развитых государств разрабатываются БПЛА-напарники (называемые также «ведомыми» или «атрибутивными») для пилотируемых самолетов тактической авиации и тяжелых БПЛА. В качестве примеров можно привести следующие подобные системы:

- «Объединенная система воздушных сил», разработанная концерном *Boeing Australia* для королевских военно-воздушных сил Австралии (рис. 1)[7];
- «Европейская межнациональная перспективная боевая авиационная система» (*FCAS*), включающая

в себя истребитель шестого поколения «Буря», атрибутивный БПЛА средней высоты и большой продолжительности полета (*MALE*) и боевое информационное облако «Связь»[8];

• атрибутивный БПЛА *XQ-58A* «Валькирия» (программа «Скайборг», США), который может выступать носителем малого автономного БПЛА «Альтиус-600», используемого для различных задач, включая РЭБ, разведку, противодействие другим БПЛА. Также может быть переоборудован для кинетического поражения воздушных и наземных целей (рис. 2)[9];

• мини-БПЛА «Ястреб», размещаемый на подвеске тяжелого БПЛА *MQ-9A* «Рипер» (разработчик — компания *General Atomics Aeronautical Systems*, США). Предназначен для разведки, наблюдения и распознавания (задача *ISR*), а также для РЭБ (рис. 3)[10].

• программа ВВС США по созданию БПЛА вертолетного типа «Будущая атака» (*FARA*) со вспомогательным БПЛА, направляемым в зоны воздействия средств ПВО противника для обнаружения, идентификации, определения местоположения и информирования о наиболее опасных комплексах, которые затем будут поражаться ВТО с основного БПЛА (рис. 4)[11]. Основное предназначение — преодоление эшелонированных систем ПВО.

Подобные БПЛА будут действовать преимущественно в составе роя, представляя сбой новый тип цели — пространственно-распределенный объект с изменяющейся структурой и возможностью перераспределения функций между отдельными элементами

Рис. 1. Атрибутивный БПЛА «Объединенная система воздушных сил» (Австралия)

Рис. 2. Атрибутивный БПЛА *XQ-58A* со вспомогательным БПЛА «Альтиус-600» (США)

Рис. 3. Вспомогательный БПЛА «Ястреб» на подвеске БПЛА *MQ-9A* (США)

Рис. 4. БПЛА «Будущая атака» со вспомогательным БПЛА (США)

в процессе выполнения задач. В качестве примера можно привести программу министерства ВВС США «Золотая Орда» — комплекс технологий для реализации совместных автономных сетевых возможностей существующих боевых беспилотных авиационных систем. Аналогичная программа существует и в Великобритании.

В зонах с высоким риском поражения возможно применение одноразовых ударных БПЛА. Фактически произойдет сращивание понятий «высокоточные авиационные средства поражения» и «одноразовые ударные БПЛА». Такие малоразмерные и малозаметные тактические единицы могут длительно барражировать в заданном районе, ведя поиск, распознавая цель для удара с последующим выбором оптимальной траектории следования к ней и совершая активное маневрирование для противодействия системам ПВО противника.

Замещение ударной пилотируемой авиации беспилотными авиационными платформами приведет к исчезновению порога допустимых боевых потерь, что существенно увеличит нагрузку на системы воздушно-космической обороны. Нападающая сторона вновь вернется к тактике массированных авиаударов, что, в свою очередь, повысит требования к информационным возможностям систем управления ПВО и средств разведки воздушных целей, пропускной способности каналов передачи данных, величине боезапаса и канальности комплексов ПВО по цели.

Тенденция исчезновения или увеличения порога допустимых боевых потерь распространится и на другие сферы вооруженной борьбы. В ее основе также будет лежать стремление вывести человека из зоны противоборства, заменив его необитаемыми образцами вооружения (автономными РТК).

Второй по значимости сферой вооруженной борьбы в войнах будущего станет, на наш взгляд, морская среда. При этом надводные и подводные корабли будут в основном применяться в качестве носителей ракетного вооружения и БПЛА. Непосредственное огневое противоборство между кораблями обретет преимущественно вспомогательный характер. В Военно-Морском Флоте по аналогии с Воздушно-космическими силами значительно увеличится доля надводных и подводных безэкипажных кораблей (БЭК), как ударных, так и обеспечивающих (разведка, РЭБ, связь, транспорт).

Корабли с экипажами станут располагаться вне зоны воздействия тактического и оперативного оружия противника, являясь центрами управления и носителями для БПЛА и легких БЭК. В морской сфере вооруженного противоборства БЭК будут, по аналогии с БПЛА в воздушной среде, образовывать многоуровневые технические экосистемы, включающие тяжелые (дорогие) и более легкие (дешевые) БЭК, а также действовать организованными группами подобно рою БПЛА. Наступательные вооружения станут устанавливать преимущественно на БЭК в целях снижения рисков нанесения противником ударов по кораблям с экипажами. В качестве примера можно привести надводный БЭК «Морской охотник», разработанный компанией «Лейдос» при поддержке агентства *DARPA* (США) (рис. 5).

Рис. 5. Надводный БЭК «Морской охотник» (США)

В Сухопутных войсках широкое распространение получат автономные и дистанционно управляемые РТК ударного и обеспечивающего (разведка, связь, РЭБ, транспорт, инженерные задачи) назначения. Огневое противоборство в наземной сфере нападающая сторона будет вести преимущественно без непосредственного участия человека с применением РТК, действующих тактическими группами.

Однако переход к наземной фазе боевых действий возможен, на наш взгляд, только на завершающей стадии конфликта, после полного достижения целей воздушно-космической наступательной операции. Они будут носить в основном локальный характер, характеризоваться низкой напряженностью и вестись в целях установления окончательного контроля (оккупации) над оспариваемой территорией, поиска и подавления отдельных очагов сопротивления противника. В качестве примера существующего многофункционального РТК военного назначения можно привести «Уран-9» (Россия), предназначенный для выполнения задач разведки и наземной огневой поддержки (рис. 6).

Рис. 6. Боевой РТК «Уран-9»

Значительно возрастут масштабы применения во всех сферах вооруженного противоборства энергетического оружия (лазерного, сверхвысокочастотного, пучкового и т. п.), мощность которого возрастет до уровня, позволяющего наносить физическое поражение различным критически важным объектам противника. Развитие технологий позволит достичь таких массогабаритных характеристик данного оружия (при сохранении требуемого уровня излучаемой мощности), которые обеспечат его высокую мобильность или транспортируемость.

Стратегическое ядерное оружие (при продолжении совершенствования его носителей) сохранит свое значение как «оружие судного дня», а тактическое, на наш взгляд, будет функционально замещено гиперзвуковыми высокоточными средствами поражения. При этом следует ожидать расширения количества держав, располагающих технологиями создания ядерных зарядов и средств их доставки.

Совершенно новую парадигму применения получат биологическое и химическое оружие, которые, вероятно, будут объединены в единый тип оружия. Современные технологии генной инженерии позволяют создавать штаммы болезнетворных микроорганизмов и вирусов, избирательно воздействующих на популяции людей с определенным генотипом, т. е. на представителей определенной расы и даже национальности. Они будут сравнительно безопасны для населения государства-агрессора, но смогут воздействовать на жителей страны-противника.

Другой возможный вариант развития технологий химико-биологического оружия — создание биологических добавок для пищевых продуктов и косметики, также избирательно воздействующих на людей с определенным генотипом, в том числе с отложенным или накопительным эффектом негативного влияния на организм человека. Подобное оружие может применяться не только против населения противника, но и для сни-

жения популяции экономически важных сельскохозяйственных культур или экологически значимых животных и растений на его территории.

Приведенные особенности химико-биологического оружия будущего позволяют изменить способ его инвазии (доставки) в популяцию потенциального противника — в условиях глобального международного рынка соответствующие вещества или микроорганизмы могут завозиться на его территорию заблаговременно (в мирное время или в угрожаемый период) в составе пищевых продуктов или через поставки зараженных сельскохозяйственных животных и растений. При этом отсутствует или значительно снижен риск поражения собственного населения и популяций сельскохозяйственных животных. Экономическое и/или эпидемиологическое ослабление государства-конкурента снизит или полностью лишит его способности сопротивляться политическому и военному давлению агрессора. Подобный сценарий применения биологического оружия против России с территории Украины готовили США.

Совершенно новую парадигму применения получат биологическое и химическое оружие, которые, вероятно, будут объединены в единый тип оружия. Современные технологии генной инженерии позволяют создавать штаммы болезнетворных микроорганизмов и вирусов, избирательно воздействующих на популяции людей с определенным генотипом, т.е. на представителей определенной расы и даже национальности. Они будут сравнительно безопасны для населения государства-агрессора, но смогут воздействовать на жителей страны-противника.

Развитие информационно-разведывательных систем и систем управления обеспечит создание глобального информационно-коммуникационного пространства. Интеграция многочисленных разведывательных систем по всему земному шару приведет к образованию глобальной информационной сети. Практически все образцы ВВСТ станут сетецентрическими. Вертикальная схема организации управления на тактическом уровне будет заменена на масштабируемую матричную и отчасти самоорганизующуюся систему, состоящую из военнослужащих, роботов и интеллектуальных подсистем. Автоматизированные системы управления (АСУ) войсками станут межвидовыми, появятся АСУ поля боя, позволяющие планировать и координировать одновременный многодоменный бой во всех сферах вооруженной борьбы на ТВД.

В качестве прообраза такого подхода можно привести американскую *IBCS* (интегрированная система боевого командования) *IAMD* (комплексная противовоздушная и противоракетная оборона) на ТВД или в районе операций объединенных сил. В перспективе совокупность интегрированных ПВО-ПРО, развернутых на ТВД и в регионах, должна составить объединенную (межвидовую) интегрированную ПВО-ПРО (*JIAMD*), способную решать весь спектр стратегических и тактических задач. В состав региональных *IAMD* предполагается включить региональные системы ПВО и ПРО, в частности, Европейскую ПРО, системы ПРО государств Азиатско-Тихоокеанского региона и Ближнего Востока.

В глобальное информационное пространство будут поступать полные сведения о противнике от всего массива разнородных разведывательных источников (технических средств разведки, агентуры, органов

войсковой разведки и др.), о состоянии и действиях своих и союзнических войск, физико-географической и климатической обстановке в районах боевых действий (метеорологической, гидрологической, радиационной и др.), а также картографические и различные справочные материалы. Туда даже будет интегрирована географическая информационная система. Всю разнородную информацию, структурированную и обобщенную при помощи специальных алгоритмов обработки сверхбольших данных, сможет получать любой потребитель, подключенный к системе при условии санкционирования соответствующего уровня доступа.

Аналогично все огневые средства и пункты управления будут включены в глобальную военную систему командования, не имеющую строгой иерархической структуры при отсутствии постоянной подчиненности средств разведки и поражения конкретным пунктам управления. В настоящее время такая концепция реализована, например, в европейском транснациональном зенитном ракетном комплексе *MEADS*[12]. Каждый командный пункт в зависимости от поставленной задачи и обстановки определяет оптимальное огневое средство (вне зависимости от видовой принадлежности) и источник информации по цели, а затем кратковременно интегрирует их в единый кластер для выполнения конкретной боевой задачи (поражения цели).

На тактическом уровне ожидается внедрение полной автоматизации управления войсками и оружием за счет применения технологий ИИ, поскольку «ручное» управление командиром (оператором) в реальном масштабе времени в большинстве случаев станет невозможным из-за высокой динамики и многофакторности боя.

На оперативном уровне АСУ, созданные на основе тех же технологий ИИ и «Большие данные», обрабатывая массивы разнородных данных, смогут эффективно осуществлять поддержку принятия решений, формируя аналитические и оперативные сводки по сложившейся обстановке, а также предлагая различные варианты решения на боевые действия с предоставлением их показателей. Боевые расчеты будут выполнять только функции планирования боевых действий и оценки их результатов, а АСУ тактического звена предстоит реализовывать принятые командованием решения при общей координации со стороны должностных лиц органов управления.

Кибероружие — приоритетное средство вооруженной борьбы в последней трети XXI века

Анализируя направленность научно-технического прогресса, можно предположить, что в последней трети XXI века произойдет глобальная цифровизация (информатизация) всех сфер общественных отношений (экономической, политической, социальной), и человечество перейдет к новой общественной формации — цифровое общество. При этом ИИ будет широко задействован не только в управлении техническими объектами, экосистемами, промышленными и другими комплексами, социальными учреждениями, но и в принятии решений по вопросам управления государством в целом. Произойдет становление электронной демократии, информационной экономики, электронного государства (электронное правительство и парламент), цифровых рынков, электронных денег, электронных социальных и хозяйствующих сетей.

В таких обстоятельствах **основная напряженность вооруженного противоборства между государствами**

На оперативном уровне АСУ, созданные на основе тех же технологий ИИ и «Большие данные», обрабатывая массивы разнородных данных, смогут эффективно осуществлять поддержку принятия решений, формируя аналитические и оперативные сводки по сложившейся обстановке а также предлагая различные варианты решения на боевые действия с предоставлением их показателей.

должна, на наш взгляд, неизбежно сместиться из воздушно-космической сферы в киберпространство. Воздействуя через киберпространство, нападающая сторона сможет достичь своих целей по парализации действий войск противника, нарушению функционирования его объектов энергетики, промышленности, транспорта, систем государственного, военного управления и связи. Это станет возможным при условии объединения систем управления критически важными объектами в единую информационную сеть и оснащения их сложным программным обеспечением, оперативный контроль функционирования которого со стороны обслуживающего и эксплуатирующего персонала невозможен.

Кибератаки на данные объекты посредством программного воздействия на их управляющие системы могут привести к разнообразным негативным последствиям, начиная от прекращения работы до аварий, в результате которых они получат физические повреждения или окажут вредное воздействие на окружающую среду. В дальнейшем все это с высокой вероятностью вызовет коллапс экономического комплекса страны, паралич работы высших звеньев управления, панику среди населения и в конечном итоге лишит государство-жертву способности организованно сопротивляться агрессору.

Возможно и более «тонкое» применение кибероружия, без изменения физического состояния атакуемых объектов. Например, воздействие на банковский сектор (частный или государственный) приведет к коллапсу систем электронных платежей и многим другим негативным последствиям, достаточным, чтобы атакуемое государство перестало быть экономическим и политическим конкурентом для агрессора.

Другим направлением использования кибероружия могут стать атаки на средства массовой информации, информационные системы и системы государственного управления, что позволит передавать ложные команды или распространять искаженную информацию, в том числе от органов государственной власти. В данном варианте происходит интеграция кибератак и информационно-психологической операции.

Информационно-психологическое воздействие на людей станет важнейшей составляющей кибервойн и будет осуществляться в целях навязывания населению атакуемого государства ложного видения характеристик мироустройства, изменения системы ценностей, мировоззрения, ментальности, поведенческих паттернов, а также его нейролингвистического программирования.

Основным объектом кибератак в войнах будущего станет преимущественно не аппаратная часть систем, поскольку она может быть полезна нападающей стороне для дальнейшего использования, а воссоздавать ее долго и дорого, а именно программное обеспечение, работоспособность которого можно быстро и дешево восстановить, особенно владея алгоритмами атакующих программ.

В связи с этим можно предположить, что инициатору войны будет невыгодно физически разрушать элементы систем связи и управления противника, поскольку это лишит его возможности применения кибероружия и ведения вооруженной борьбы в киберпространстве в целом. Такой подход находит свое подтверждение в сегодняшнем глобальном противостоянии России с Западом, когда США вывели из-под санкций поставки в РФ телекоммуникационного и интернет-оборудования.

Кибероперации, как и информационно-психологические операции, начнут проводиться еще до начала открытых боевых действий, в период обострения обстановки. С высокой вероятностью противоборство в киберсфере между государствами-конкурентами будет вестись перманентно, в том числе и в мирное время, поскольку факт кибератаки сложно оперативно обнаружить, а ее источник непросто доказательно установить. Произойдет фактическое размывание временнóй границы начала войны, будет иметь место постоянное воздействие «небоевым» оружием на государства-конкуренты, в том числе в мирное время.

Кроме внедрения кибероружия в последней трети XXI века возможны и другие значительные тенденции развития средств вооруженной борьбы и способов их применения. В частности, следует, на наш взгляд, ожидать интеграцию биологических и небиологических технологий в образцах ВВСТ (создание киберорганических объектов) с возможностью их самовосстановления, реконфигурации и динамического изменения формы, а также внедрение нановооружений («умной пыли»), т. е. искусственных объектов сверхмалых размеров (порядка микрометров) биологической или технической природы, применяемых в интересах решения задач вооруженного противоборства.

На основе изложенного можно утверждать, что **войны будущего будут характеризоваться следующими основными чертами**:

• сетецентричностью;

• доминированием воздушно-космической сферы вооруженного противоборства с постепенным возрастанием роли и значения киберпространства;

• выводом боевых расчетов (экипажей) из зон воздействия оперативного и тактического оружия противника;

• высокой степенью роботизации, автоматизации и интеллектуализации образцов ВВСТ;

• широким применением технологий ИИ при планировании боевых действий, управлении войсками и оружием;

• высокой значимостью систем управления оружием, формированием глобального информационного пространства и появлением многодоменных АСУ, позволяющих одновременно управлять боевыми действиями во всех сферах вооруженной борьбы;

• сбережением инфраструктуры и окружающей среды оспариваемой территории (пространства);

Основная напряженность вооруженного противоборства между государствами должна, на наш взгляд, неизбежно сместиться из воздушно-космической сферы в киберпространство. Воздействуя через киберпространство, нападающая сторона сможет достичь своих целей по парализации действий войск противника, нарушению функционирования его объектов энергетики, промышленности, транспорта, систем государственного, военного управления и связи.

- постепенным исчезновением границ между военным и мирным временем.

В заключение необходимо отметить, что наиболее вероятным сценарием развития военно-политической обстановки в мире становится нарастание глобальных противоречий между ведущими государствами, и война (вооруженная борьба) останется одним из основных потенциальных методов их разрешения. При этом влияние последствий войны на экологическую ситуацию не позволит остаться в стороне даже государствам, непосредственно в вооруженном противоборстве не участвующим.

Научно-технический прогресс по-прежнему будет непрерывно и принципиально менять не только облик средств вооруженной борьбы, но и характер будущих войн. Несмотря на их кажущуюся гуманизацию, воздействие вооруженной борьбы на население не станет менее катастрофичным. Более того, от поражения перспективным оружием невозможно защититься расстоянием, поскольку удары будут наноситься по всей территории воюющих государств и планеты в целом, а первоочередными целями станут не группировки войск (сил), а объекты инфраструктуры и само население.

Наряду с этим следует иметь в виду, что одной из значимых тенденций развития военно-политической обстановки в мире становится размывание грани между миром и войной как состояниями общества и межгосударственных отношений. В перспективе вооруженное и невооруженное противоборство будут малоразличимы как по способам ведения, так и по результатам воздействия.

ПРИМЕЧАНИЯ

[1] *Харари Ю.Н.* Sapiens. Краткая история человечества. М.: Синдбад, 2011. 516 с.

[2] Владимир Путин принял участие в пленарной сессии XVIII заседания Международного дискуссионного клуба «Валдай». 21 октября 2021. URL: http://kremlin.ru/events/president/news/66975 (дата обращения: 28.03.2022).

[3] *Харари Ю.Н.* Краткая история будущего. М.: Синдбад, 2019. 492 с.

[4] *Харари Ю.Н.* 21 урок для XXI века. М.: Синдбад, 2019. 412 с.

[5] Там же.

[6] *Каку М.* Физика будущего. М.: Альпина нон-фикшн, 2016. 584 с.

[7] FlightGlobal: Boeing Australia, RAAF fly second ATS loyal wingman. 2021. URL: https://www.flightglobal.com/military-uavs/boeing-australia-raaf-fly-second-ats-loyal-wingman/146253.article (дата обращения: 05.11.2021).

[8] Janes: FCAS/SCAF partner nations launch NGF demonstrator phase. 2021. URL: https://www.janes.com/defence-news/news-detail/fcasscaf-partner-nations-launch-ngf-demonstrator-phase (дата обращения: 17.05.2021).

[9] Janes: US Air Force completes XQ-58A Valkyrie's first payload release test. 2021. URL: https://www.janes.com/defence-news/news-detail/update-us-air-force-completes-xq-58a-valkyries-first-payload-release-test, (дата обращения: 12.04.2021).

[10] Janes: GA-ASI reveals Sparrowhawk air-launched and air-recoverable UAV. 2020. URL: https://www.janes.com/defence-news/news-detail/ga-asi-reveals-sparrowhawk-air-launched-and-air-recoverable-uav (дата обращения: 10.11.2021).

[11] FlightGlobal: US Army to exploit crucial weakness in Russian, Chinese air defences. 2020. URL: https://www.flightglobal.com/helicopters/us-army-to-exploit-crucial-weakness-in-russian-chinese-air-defences/140311.article (дата обращения: 13.10.2021).

[12] Jane's Land Warfare Platforms. Artillery & Air Defense. 2020—2021. Mark Cazalet, Sunil Nair, Jon Hawekes. 1000 p.

Состояние и основные направления развития автоматизированных систем управления радиоэлектронной борьбой

Генерал-майор А.Д. СИМОНОВ

АННОТАЦИЯ

Представлены результаты ретроспективного анализа развития автоматизированных систем управления радиоэлектронной борьбой и на их основе сформулированы ключевые направления развития АСУ РЭБ на основе внедрения современных информационных технологий, включая технологии искусственного интеллекта.

ABSTRACT

The paper presents the results of retrospective analysis of progress in automated control systems (ACS) for electronic warfare, and formulates on this basis key EW ACS development trends that rely on modern IT introduction, including artificial intelligence technologies.

КЛЮЧЕВЫЕ СЛОВА

Радиоэлектронная борьба, автоматизированная система управления (АСУ), интеллектуализация.

KEYWORDS

Electronic warfare, automated control system, automation equipment set, intellectualization.

МАГИСТРАЛЬНЫМ направлением развития современных автоматизированных систем управления радиоэлектронной борьбой является внедрение передовых информационных технологий, в том числе с применением элементов искусственного интеллекта, на всех уровнях системы управления войсками РЭБ и интеграция в единый контур управления войсками (силами) и оружием в составе АСУ Вооруженных Сил Российской Федерации.

Современный этап развития радиоэлектронной борьбы характеризуется перерастанием ее из вида боевого и оперативного обеспечения в непосредственное содержание ведения военных действий, существенным возрастанием значимости РЭБ как одного из эффективных, быстро реализуемых и экономически предпочтительных способов нейтрализации преимуществ развитых иностранных государств в области создания интегрированных информационно-управляющих систем. В условиях возрастания динамики боевых действий, увеличения номенклатуры и возможностей существующей и перспективной техники радиоэлектронной борьбы для достижения требуемого уровня планирования мероприятий и действий войск (сил и средств) РЭБ, обеспечения оперативного управления ими при выполнении всего комплекса задач РЭБ в космическом, воздушном, наземном пространстве и на морских акваториях необходимы сквозная комплексная автоматизация процессов управления радиоэлектронной борьбой, оснащение органов (пунктов) управления РЭБ всех звеньев комплексами средств автоматизации (КСА), реализующими перспективные компьютерные технологии поддержки принятия решений по РЭБ.

Ретроспективный анализ состояния и результатов выполненных работ в области автоматизации управления радиоэлектронной борьбой в Вооруженных Силах Российской Федерации, оснащения органов (пунктов) управления РЭБ различных звеньев комплексами средств автоматизации показал, что в целом развитие и совершенствование указанных КСА не отличается от общемировых тенденций развития корпоративных информационно-расчетных систем и происходит в направлениях расширения их функциональных возможностей и состава поддерживаемых функций управления.

Не останавливаясь детально на этапе зарождения процессов автоматизации управления радиоэлектронной борьбой в 1980—1990-е годы (автономный автоматизированный пункт управления РЭБ фронта (армии) «Салгир-7Ф(А)», КСА в составе АСУ войсками фронта (армии) «Маневр», АСУ войсками стран Варшавского договора «Авангард», КСА службы РЭБ штаба фронта в составе АСУ «Искра» и т. д.), следует признать, что настоящим прорывом в области развития автоматизированных систем управления в частях РЭБ явилось принятие на вооружение в 1999 году автоматизированного командного пункта (АКП) отдельного батальона РЭБ армии РП-300КП («Реактор-1»).

В этом изделии впервые был реализован ряд новых технических решений, ставших теперь стандартными для нового поколения техники автоматизированного управления радиоэлектронной борьбой. Изделие оснащалось новейшими для того времени средствами вычислительной техники, навигационной аппаратурой. Автоматизированные рабочие места лиц оперативного состава АКП были объединены в локальную вычислительную сеть. Был реализован автоматический прием и запись в базу данных информации от подчиненных подразделений, взаимодействующих частей и вышестоящих органов управления. Решение информационных и расчетных задач по РЭБ производилось на фоне электронной карты местности с использованием цифровой картографической информации.

Ретроспектива развития КСА органов управления РЭБ представлена на рисунке.

В настоящее время работы в области автоматизации процессов управления радиоэлектронной борьбой ведутся на всех уровнях системы

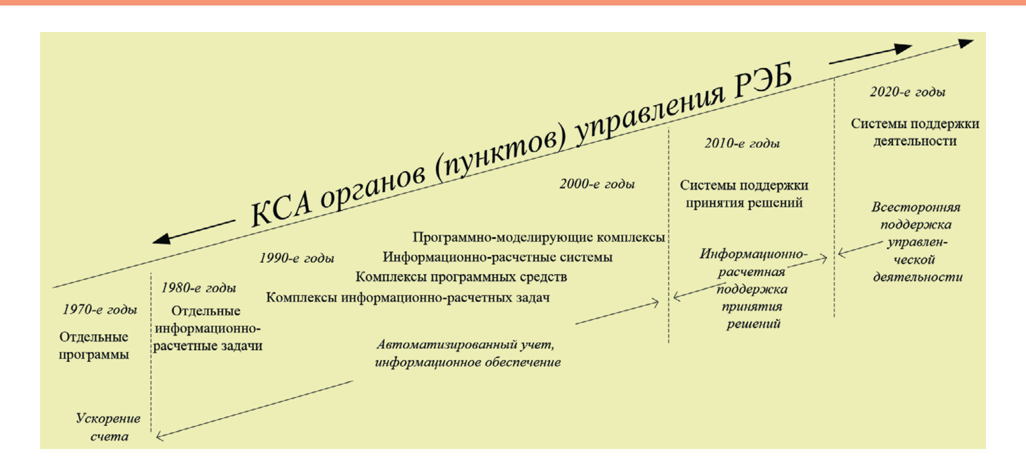


Рис. Ретроспектива развития КСА органов управления РЭБ

управления войсками РЭБ. Они носят комплексный характер и предусматривают:

• переход на использование в технике автоматизированного управления радиоэлектронной борьбой унифицированных отечественных аппаратно-программных платформ;

• объединение комплексов средств автоматизации органов (пунктов) управления РЭБ всех звеньев, АКП соединений (частей, подразделений) РЭБ в единую АСУ войск РЭБ, ее интеграцию в Единое информационное пространство (ЕИП) Вооруженных Сил РФ;

• расширение состава автоматизированных функций управления должностных лиц органов (пунктов) управления РЭБ, АКП соединений (частей, подразделений) РЭБ, функционирующих в едином контуре управления;

• внедрение перспективных информационных технологий в процессы сбора, обработки, накопления, хранения, поиска и выдачи по запросам, представления и передачи информации (данных оперативной и радиоэлектронной обстановки).

Работы по переходу техники РЭБ на отечественное аппаратное и программное обеспечение направлены в первую очередь на исключение зависимости от зарубежных компьютерных технологий. В части программного обеспечения удалось достичь определенных успехов: практически вся современная техника РЭБ функционирует на базе отечественных операционных систем. В части аппаратного обеспечения завершается создание единого типоряда (типажа) отечественных аппаратных платформ для вооружения, военной и специальной техники, что позволит начиная с 2023 года осуществлять плановое переоснащение на эти платформы существующей и перспективной техники РЭБ.

Работы по формированию Единого информационного пространства войск РЭБ и его интеграции в ЕИП Вооруженных Сил РФ были начаты в начале 2000-х годов с принятием Концепции Единого информационного пространства Вооруженных Сил Российской Федерации. За прошедшие годы систематизированы и актуализированы информационные ресурсы войск РЭБ: словарно-терминологическая основа, унифицированные формы документов, необходимая нормативно-справочная информация, каталоги (библиотеки) электронных условных знаков (в части РЭБ) и др. Функционирует служба информационных ресурсов. Делаются практические шаги по созданию центров

обработки данных, содержащих информационные фонды, и организации доступа к ним заинтересованных должностных лиц. Важным этапом создания единого информационного пространства, повышения уровня информационной обеспеченности актуальными данными оперативной и радиоэлектронной обстановки органов (пунктов) управления РЭБ всех звеньев является организация информационно-технического взаимодействия АСУ войск РЭБ с АСУ видов, родов войск Вооруженных Сил Российской Федерации, органов военного и государственного управления. В стратегическом и оперативном звеньях (военный округ — армия) эта задача успешно решается благодаря единому разработчику КСА для органов (пунктов) управления РЭБ. Названные КСА построены на основе однотипного (унифицированного) общего и общесистемного программного обеспечения, имеют единую информационно-моделирующую среду, реализуют доступ к единым базам данных, обеспечивают геоинформационную поддержку, что снимает практически любые ограничения при информационном взаимодействии АСУ РЭБ с другими автоматизированными системами в этих звеньях управления как «по горизонтали», так и «по вертикали».

Основной отличительной чертой современных и перспективных автоматизированных систем управления РЭБ является переход от технологий простых информационно-расчетных систем к технологиям комплексной поддержки принятия решений по РЭБ, сопровождающийся увеличением степени автоматизации процессов управления подчиненными войсками (силами и средствами) РЭБ. В современных КСА это увеличение достигается не на количественном, а на качественном уровне, главным образом за счет реализации контуров автоматизированного управления на всех этапах организации РЭБ в операциях (военных действиях) и непосредственного управления силами и средствами РЭБ в ходе их ведения. При этом обеспечивается непрерывная поддержка принятия решений должностными лицами органов (пунктов) управления РЭБ на всех этапах их работы. В названных КСА реализуются современные технологии сбора, обобщения, хранения, поиска, представления, передачи информации, позволяющие практически в реальном времени и в полном объеме обеспечить поддержку процессов принятия решений.

Важнейшим направлением развития и совершенствования АСУ войск РЭБ является внедрение в программное обеспечение их КСА технологий искусственного интеллекта. В основу работ по интеллектуализации АСУ войск РЭБ положены решения, принятых как на государственном уровне[1], так и на уровне Министерства обороны Российской Федерации. В октябре 2019 года принята «Национальная стратегия развития искусственного интеллекта на период до 2030 года», организована работа Военно-промышленной комиссии Российской Федерации в данном направлении, в Министерстве обороны создана Дирекция по вопросам развития и внедрения технологий искусственного интеллекта в образцы вооружения, военной и специальной техники. В соответствии с перечнем поручений Министра обороны Российской Федерации создается сеть подразделений, отвечающих за научную проработку и обоснование применения технологий искусственного интеллекта в перспективных образцах вооружения. Практическая реализация требований руководящих документов в данной области применительно к технике РЭБ обеспечивается включением в тактико-тех-

нические задания на задаваемые опытно-конструкторские работы требований по использованию технологий искусственного интеллекта.

Первоочередными задачами, решаемыми с применением названных технологий, являются для:

- автоматизированных систем управления войсками (силами и средствами) РЭБ Вооруженных Сил Российской Федерации — поддержка принятия решений органами управления РЭБ на всех этапах подготовки и ведения РЭБ в операциях (военных действиях) с применением методов экспертных систем, интеллектуального анализа данных большого объема, извлечения знаний из различных источников;
- автоматизированных командных пунктов соединений и частей РЭБ — комплексное целераспределение сил и средств РЭБ наземного и воздушного базирования на разведку и подавление на основе применения искусственных нейронных сетей и генетических алгоритмов, а также методов машинного обучения;
- наземных комплексов радиоэлектронного подавления и комплексов на беспилотных летательных аппаратах, а также комплексов специального воздействия — обработка разведывательной информации, целераспределение и целеуказание объектов РЭБ с использованием методов нечеткой логики, искусственных нейронных сетей, алгоритмов автоматизированных непилотируемых интеллектуальных систем;
- комплексов защиты объектов от высокоточного оружия — адаптивное снижение заметности объектов, реализация технических решений, минимизирующих отраженный сигнал, на основе применения методов экспертных систем и искусственных нейронных сетей;
- комплексов обеспечения испытаний техники РЭБ — обоснование рациональных способов воспроизведения радиоэлектронной обстановки, соответствующей ожидаемой реальной, путем использования методов компьютерного зрения, распознавания и синтеза речи, а также методов экспертных систем;
- тренажерных систем РЭБ — моделирование процессов обучения, воспроизведение оперативной и радиоэлектронной обстановки с использованием технологий виртуальной реальности, автоматический подбор рациональных стратегий обучения на основе использования динамических развивающихся баз знаний, автоматического учета новой информации.

В настоящее время активно ведутся работы по созданию систем поддержки принятия решений (СППР) с элементами искусственного интеллекта для КСА органов (пунктов) управления РЭБ различных звеньев. Особенности организации и выполнения таких работ характеризуются следующим.

Первое. Реализуется принцип «необходимости и достаточности». Накопленный организациями промышленности опыт разработки специального программного обеспечения для КСА органов (пунктов) управления РЭБ различных звеньев однозначно указывает на пагубность попыток максимально формализовать действия должностных лиц. Все формализовать невозможно, и в условиях динамично меняющейся обстановки должностные лица органов (пунктов) управления РЭБ должны иметь определенную свободу действий, возможность принимать нестандартные решения. Излишняя формализация процессов этому только мешает.

Второе. Соблюдается принцип (сформулированный Саридисом в 1989 году для интеллектуальных систем[2]), заключающийся в том, что по

мере продвижения от низших к высшим уровням иерархической системы управления уровень и сложность выполняемых задач повышаются, в то время как точность расчетов, принимаемых решений и вырабатываемых на их основе рекомендаций, наоборот, снижается. Это обусловлено кратным возрастанием объемов информации, обрабатываемой на верхних уровнях иерархии системы управления, а также возрастанием при этом в общем информационном потоке доли плохо формализуемой и слабоструктурированной информации.

Третье. Применение технологий искусственного интеллекта, в силу их особенностей и возможностей, ориентировано в первую очередь на принятие решений на основе слабоструктурированных и неструктурированных исходных данных по РЭБ. Это предполагает:

• отказ от упрощенных моделей процессов управления (типа моделей состояний, вероятностных описаний, игр автоматов со средой и т. д.) и обеспечение тесного информационного взаимодействия управляющих систем с управляемыми процессами;

• наличие нескольких уровней самонастройки, самоорганизации и самообучения;

• реализации алгоритмов прогнозирования изменений оперативной и радиоэлектронной обстановки и собственного (сил и средств РЭБ) поведения в ней;

• сохраняемости функционирования при разрыве иерархических связей в системе управления.

Четвертое. Соблюдается принцип преемственности. Системы поддержки принятия решений для органов (пунктов) управления РЭБ различных звеньев на основе технологий искусственного интеллекта относятся к классу сложных систем. Это требует для их разработки и внедрения определенного времени. Такие системы никогда не создаются «с нуля», они всегда являются развитием созданных и апробированных ранее систем меньшего уровня сложности, аккумулируют ранее разработанные и апробированные технические и программные решения. Но и прирост эффективности автоматизированного управления войсками (силами и средствами) РЭБ, в особенности в условиях динамичной, быстроменяющейся обстановки, характеризующейся высокой степенью неопределенности, ожидается существенный.

Таким образом, в настоящее время идет интенсивный процесс развития и совершенствования автоматизированных систем управления радиоэлектронной борьбой. Внедрение новых информационных технологий, унификация аппаратного и программного обеспечения таких АСУ, их интеграция в единый контур управления войсками и оружием, внедрение новых информационных технологий, и в первую очередь технологий искусственного интеллекта, позволят существенно повысить эффективность управления войсками (силами и средствами) РЭБ и в конечном итоге увеличить вклад войск РЭБ в завоевание превосходства над противником в управлении войсками (силами) и оружием.

ПРИМЕЧАНИЯ

[1] Указ Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» от 10 октября 2019 г.

[2] *Шпак В.Ф.* Информационные технологии в системе управления ВМФ (теория и практика, состояние и перспективы развития / В.Ф. Шпак, Н.Ф. Директоров, В.И. Мирошников, С.Н. Навойцев, В.Н. Наумов, А.В. Серегин, Ю.И. Синещук, О.М. Туровский; под общ. ред. В.В. Авдошина. СПб.: Элмор, 2005. 832 с.

Методологические подходы к оценке эффективности системы связи тактического звена управления

Полковник И.Г. ВОРОБЬЁВ,
кандидат военных наук

Полковник В.М. РОМАНОВ

Майор М.А. ПОПОВА

АННОТАЦИЯ

Изложены базовые основы методологии оценки системы связи, предложен метод нормативного прогнозирования информационной нагрузки, поступающей на систему связи, и нормированной оценки возможностей противника по воздействию на систему связи. Представлены подходы к оценке эффективности системы связи на основе оценки важности сетевых элементов.

КЛЮЧЕВЫЕ СЛОВА

Эффективность системы связи, информационный трафик, нормативный метод.

ABSTRACT

The paper goes over the basic foundations of assessment methodology for the communication system, suggesting the method of normative prognostication for the communication system information load and normalized assessment of the adversary's ability to affect the communication system. It gives approaches to the communication system efficiency estimation on the basis of assessing the importance of network elements.

KEYWORDS

Communication system efficiency, information traffic, normative approach.

ОЦЕНКА эффективности систем военной связи в современных условиях является обязательным этапом аналитической работы органов управления связью. Эта задача может решаться как при организации связи в ходе подготовки к ведению боевых действий, так и при оперативном управлении действующей связью в ходе выполнения боевых задач.

Методология оценки эффективности системы связи представляет собой совокупность принципов, которыми руководствуются органы управления связью при обосновании решений на построение системы связи, а также методов и методик ведения аналитической работы. Ключевыми методологическими аспектами решения данной задачи являются: определение исходных данных, задание системы показателей и критериев оценки эффективности, а также выбор метода решения задачи многокритериальной оценки вариантов построения системы связи. Результатом оценки эффективности системы связи тактических формирований

должно быть определение «вклада» системы связи в эффективность системы управления войсками.

Как информационную систему, систему управления войсками характеризует информационная структура, представляющая собой совокупность информационных направлений с характеристиками циркулирующей в них информации? Под информационным направлением понимается направление обмена информацией между пунктами управления (отдельными должностными лицами), характеризуемое степенью важности, видом и объемом передаваемой информации, а также интенсивностью и режимом обмена информацией. Важность информационного направления напрямую зависит от качественных показателей передаваемой (принимаемой) информации. Для обеспечения передачи всех видов информации на информационных направлениях развертываются направления связи.

При проведении оперативных расчетов принято, что система управления функционирует устойчиво при передаче не менее 80 % необходимого объема информации, управление затруднено при своевременной передаче не менее 60 % требуемой информации, управление нарушено при снижении информационного обмена до 40 % и сорвано при передаче менее 20 % информации (табл. 1)[1,2].

Таблица 1

Зависимость состояния управления войсками от объема передаваемой информации

Состояние управления войсками	Объем информации, передаваемой в системе связи, % от заданного			
	Всего	1-й приоритет	2-й приоритет	3-й приоритет
Устойчивое	80—100	100	100	50—100
Затруднено	60—80	100	100	10—20
Нарушено	20—60	100	80—100	0
Сорвано	Менее 20	Менее 20	0	0

Традиционный подход к оценке систем связи предполагает определение путем проведения статистических исследований поступающей информационной нагрузки; задание требований к вероятностно-временным характеристикам предоставления услуг связи на направлениях связи, моделирование элементов системы связи системами массового обслуживания, расчет вероятности своевременности доставки сообщений на направлениях связи; сравнение полученных результатов с требованиями и принятие решения по состоянию системы связи. При проведении практических расчетов такой подход трудно выполним из-за наличия следующих методологических проблем.

Главной и на настоящий момент не решенной методологической проблемой является определение показателей прогнозируемого информационного трафика, циркулирующего в системе управления войсками. Трафик информации в системе управления соединения определяют: структура системы пунктов управления; состав и количество информационных направлений; динамика перемещения элементов системы управления; количество должностных лиц

пункта управления, рабочих групп; возложенные на органы управления функции управления, решаемые должностными лицами задачи в ходе ведения боевых действий; количество и тактико-технические характеристики средств управления и связи, а также другие трудно формализуемые, в том числе и психологические факторы. Выделим ключевые особенности прогнозирования информационной нагрузки в системах связи тактического звена управления.

Под информационным направлением понимается направление обмена информацией между пунктами управления (отдельными должностными лицами), характеризуемое степенью важности, видом и объемом передаваемой информации, а также интенсивностью и режимом обмена информацией. Для обеспечения передачи всех видов информации на информационных направлениях развертываются направления связи.

Прежде всего необходимо отметить, что системы связи тактических формирований, как правило, создаются для решения задач в течение ограниченного интервала времени, что не позволяет собрать достоверную статистику по информационной нагрузке. В то же время провести эксперимент (опытные учения) с целью сбора статистического материала также сложно, так как невозможно воссоздать конкретные условия функционирования системы управления войсками. Чрезвычайная сложность ряда прогнозируемых процессов и априорная неопределенность многих исходных данных, как то: изменение в динамике боевых действий приоритетности информационных направлений и объема передаваемых сообщений — делают процесс прогнозирования информационного трафика неразрешимой проблемой. В связи с вышеперечисленными особенностями прогнозирования характеристик информационных направлений имеющиеся в настоящее время данные по объему и интенсивности информационных потоков обладают высокой степенью неопределенности.

Особенностью систем связи военного назначения является потенциальная возможность административного ограничения доступа к ресурсу сети связи. Это обстоятельство предопределяет широкое использование нормативных методов прогнозирования и определения параметров информационного трафика. Нормативный метод опирается на сочетание математического и эмпирико-эвристического прогнозирования в целях создания норм на возможности использования сети связи тактического формирования. Потребности в услугах связи могут нормироваться как по группам пользователей, так и по информационным направлениям. При проведении нормативного прогноза используются, как правило, экспертные методы. Методические подходы к составлению нормативного прогноза информационной нагрузки представлены в работе И.Г. Воробьева «Управление трафиком…»[3]. Следует отметить, что заданные нормы на предоставление услуг связи целесообразно задавать на пятилетний срок.

Проблема отсутствия статистических данных характерна и при оценке возможностей противника по воздействию на систему связи. При решении данной задачи также целесообразно задавать нормированные показатели, учитывающие состояние средств разведки и поражения противника, их боевой порядок, алгоритмы и тактику действий. Необходимо

определять уровень развития противостоящего противника и нормированные значения показателей воздействия.

При решении данной задачи предлагается следующий подход. Район обеспечения связи разбивается на зоны, для которых определяются соответствующие коэффициенты поражаемости.

К примеру, оценка устойчивости узлов связи может осуществляться с учетом продолжительности ведения боевых действий (планируемого применения), места размещения (развертывания), степени подвижности и возможностей противника по воздействию на систему и войска связи, при этом рассчитывается коэффициент выживаемости по формуле:

$$К_{выж} = 1 - К_{пор1}К_{пор2}К_{пор3}К_{пор4}, \qquad (1)$$

где: $К_{пор1}$ — коэффициент поражаемости, зависящий от продолжительности ведения боевых действий (табл. 2);

$К_{пор2}$ — коэффициент поражаемости, зависящий от подвижности узлов связи (табл. 3);

$К_{пор3}$ — коэффициент поражаемости, зависящий от места размещения (развертывания) узла связи (табл. 4);

$К_{пор4}$ — коэффициент поражаемости, зависящий от возможностей противника по воздействию на систему и войска связи (табл. 5).

Таблица 2

Значения коэффициента поражаемости, зависящего от продолжительности ведения боевых действий

Продолжительность боевых действий (сутки)	Коэффициент поражаемости
1	0,1
2	0,15
3	0,2
4	0,25
5	0,3
6	0,35
7	0,4

Таблица 3

Значения коэффициента поражаемости, зависящего от подвижности узлов связи

Подвижность УС	Коэффициент поражаемости
Стационарный	0,9
Полевой 1 раз в 3 суток	0,8
Полевой 1 раз в 2 суток	0,7
Полевой 1 раз в 1 сутки	0,6
Полевой 2 раза в сутки	0,5
Полевой 3 раза в сутки	0,4

Таблица 4

Значения коэффициента поражаемости, зависящего от места размещения (развертывания) узла связи

Размещение	Коэффициент поражаемости
На направлении главного удара противника в тыловой зоне	0,7
На направлении главного удара противника в передовой зоне	0,9
На направлении другого удара противника в тыловой зоне	0,5
На направлении другого удара противника в передовой зоне	0,6

Таблица 5

Значения коэффициента поражаемости, зависящего от возможностей противника по воздействию на систему и войска связи

Характеристика противника	Коэффициент поражаемости
Сильный	1
Средний	0,9
Слабый	0,7

Устойчивость линий связи зависит от степени выживаемости узлов связи, между которыми организована линия связи, технической надежности (коэффициент готовности), коэффициента поражаемости линии связи средствами РЭБ.

Приемлемость того или иного решения на связь обусловливается величиной показателя эффективности, достигаемой системой связи в случае его реализации. Показатель эффективности выражает степень выполнения системой связи стоящей задачи с учетом требований, предъявляемых к системе в рассматриваемых условиях обстановки. Решение задач развертывания, усиления и наращивания системы связи оценивается показателями структурной эффективности (Эс), а задач доставки сообщений по элементам системы — показателями функциональной эффективности (Эф). Оценка структурной эффективности основывается на учете свойств сил и средств связи, используемых в элементах системы связи — линиях связи и сетях связи. Оценка функциональной эффективности основывается на учете свойств сообщений, доставляемых по этим элементам (нормированного информационного трафика). Свойства, присущие силам и средствам связи тактических формирований, относятся к структурным и являются свойствами системы связи. Свойства, присущие сообщениям, относятся к функциональным и характеризуют связь — процесс доставки сообщений. Определенным условиям обстановки будут соответствовать определенные свойства системы связи и информационного обмена. В ходе боевых действий система связи будет подвергаться разведке со стороны противника, наносимым им ударам, создаваемым помехам, а также случайным воздействиям природной среды.

Оценка эффективности системы связи может производиться по одной или нескольким тактическим задачам, по отношению к одному элементу системы или их совокупности, применительно к простым или сложным условиям обстановки. Поэтому она должна быть системной и комплексной. Системность оценки базируется на учете эффективности всех элементов системы связи и их важности в каждой из выполняемых ею задач. Комплексность оценки основывается на учете всех структурных и функциональных свойств, описывающих систему связи в рассматриваемых условиях выполнения тактических задач.

Исходя из особенностей организации связи, обоснование решений осуществляется на основе применения метода детерминированного планирования по вариантам, согласно которым рассмотрению подлежит множество рациональных вариантов построения и применения системы связи в конкретных условиях обстановки. Рациональным считается вариант построения системы связи, значения показателей эффективности которого соответствуют требованиям. По соотношению показателей структурной и функциональной эффективности можно судить о рациональности рассматриваемой системы связи. Из множества рациональных вариантов выбирается оптимальный (предпочтительный) по экстремальному значению главного показателя эффективности либо требующий на свою реализацию минимум расхода сил и средств. Поскольку решения на связь принимаются, как правило, исходя из определенного состава сил и средств связи, то их оптимизация по затратам имеет смысл главным образом в задачах долгосрочного развития системы связи.

Предлагаемые для практического применения методики оценки эффективности позволяют быстро и просто получить объективное представление о последствиях принимаемых решений на построение и использование систем военной связи применительно к прогнозируемым условиям обстановки. Объективность результатов оценки эффективности рассматриваемой системы связи будет зависеть в основном от достоверности используемых исходных данных и ошибок, допускаемых при проведении расчетов.

Методика позволяет произвести интегральную оценку эффективности системы связи, т. е. системно и комплексно оценить структурную и функциональную эффективность системы, с тем чтобы можно было выявить ее уязвимые места и определить наиболее приемлемые пути их устранения.

В методике оценки эффективности системы связи сначала определяется структурная и функциональная эффективность задействованных в каждом информационном направлении связи линий и путей связи, затем соответствующие эффективности направлений связи и исходя из них эффективности системы связи.

Эффективность линии (пути) связи определяется по формуле:

$$\text{Э}_{\text{л(п)с}}^{\text{с(ф)}} = 1 - nN^{-1} \text{ при } \text{К}_{\text{выж}} \geq \text{К}_{\text{выж}}^{\text{тр}}, n < N, \quad (2)$$

где: $\text{Э}_{\text{л(п)с}}^{\text{с(ф)}}$ — структурная (функциональная) эффективность линии (пути) связи;

N — при оценке структурной эффективности — количество объектов связи, входящих в состав линии (пути); при оценке функциональной

эффективности — количество сообщений, поступающих в линию (путь) связи;

n — при оценке структурной эффективности — количество объектов связи, а при оценке функциональной эффективности — количество сообщений, показатели качества которых не отвечают предъявляемым требованиям;

$K_{выж}$, $K^{тр}_{выж}$ — показатели качества — реальный и требуемый: при оценке структурной эффективности характеризуют качество объектов связи.

Эффективность направления связи определяется по формуле:

$$Э^{с(ф)}_{НС} = \sum_{i=1}^{m} Э^{с(ф)}_{л(п)с_i} В_{л(п)с_i}, \qquad (3)$$

где: $i = 1,2,\ldots,m$ — количество линий и путей в направлении связи;

$В_{л(п)сi}$ — важность линии (пути) связи.

При использовании этой формулы предполагается, что разные линии и пути связи для одновременной доставки одних и тех же сообщений не используются.

Эффективность направлений связи, организуемых от пункта управления, в рассматриваемой тактической задаче определяется по формуле:

$$Э^{с(ф)}_{ССПУ} = \sum_{j=1}^{n} Э^{с(ф)}_{НС_j} В_{НС_j}, \qquad (4)$$

где: $j = 1,2,\ldots,n$ — количество направлений в составе системы связи;

$В_{НС}$ — важность направления связи.

Важность элементов системы связи рассчитывается с учетом тактической важности обеспечиваемых ими информационных направлений, а также количества и видов предоставляемых для управления войсками (их взаимодействия) каналов связи.

Тактическая важность информационного направления соответствует важности того войскового формирования, на которое оно организовано и, в свою очередь, определяет важность обеспечивающего его работу направления связи. Тактическая важность войскового формирования будет определяться количеством входящих в него и предназначенных для выполнения тактической задачи условных боевых единиц, соотнесенных с их общим количеством в рассматриваемой группировке войск.

Тактическая важность направления связи определяется по формуле:

$$В_{НС} = В_{ИН} = У_{ВФ} У^{-1}_{ГВ} \text{ при } \sum_{j=1}^{n} В_{НС_i} = 1, \qquad (5)$$

где $j = 1,2,\ldots,n$ — количество направлений связи в составе системы связи пункта управления;

$У_{ВФ}$, $У_{ГВ}$ — количество задействованных условных боевых единиц в рассматриваемом войсковом формировании и группировке войск соответственно.

Важность линии (пути) связи будет зависеть от тактической важно-

Нормативный метод опирается на сочетание математического и эмпирико-эвристического прогнозирования в целях создания норм на возможности использования сети связи тактического формирования. При проведении нормативного прогноза используются, как правило, экспертные методы.

сти обеспечиваемого направления связи, канальных емкостей этого направления и линии (пути) связи, приведенных к требуемой канальной емкости информационного направления.

Канальная емкость линии (пути) связи будет определяться минимальной канальной емкостью входящих в нее (него) участков связи. Определяем относительную канальную емкость линии (пути) связи по следующей формуле:

$$Q_{\text{л(п)с}}^{\text{отн}} = Q_{\text{л(п)с}} Q_{\text{ин}}^{\text{тр}^{-1}} \text{ при } \mathrm{Q}_{\text{л(п)с}} = \min Q_{\text{уч}}, \quad (6)$$

где: $Q_{\text{л(п)с}}$ — канальная емкость линии (пути) связи, измеряемая количеством типовых каналов передачи;

$Q^{\text{тр}}_{\text{ИН}}$ — требуемая канальная емкость информационного направления;

$Q_{\text{уч}}$ — канальная емкость участка линии (пути) связи.

После этого рассчитывается важность линии (пути) связи:

Определенным условиям обстановки будут соответствовать определенные свойства системы связи и информационного обмена. В ходе боевых действий система связи будет подвергаться разведке со стороны противника, наносимым им ударам, а также случайным воздействиям природной среды.

$$\mathrm{B}_{\text{л(п)с}} = \mathrm{B}_{\text{НС}} Q_{\text{л(п)с}}^{\text{отн}} \left(\sum_{i=1}^{m} Q_{\text{л(п)с}_i}^{\text{отн}}\right)_{\text{НС}}^{-1}, \quad (7)$$

при

$$\sum_{i=1}^{m} \mathrm{B}_{\text{л(п)с}_i} = \mathrm{B}_{\text{НС}}$$

где m — количество линий (путей) в направлении связи.

Все объекты связи ранжируются по обслуживаемым ими линиям (путям) связи, организуемым в информационных направлениях.

Знание «веса» объекта позволяет определить потерю эффективности системы связи по пропускной способности при его выходе из строя. Заблаговременная оценка важности каждого из объектов системы связи дает возможность быстрого определения ее эффективности при поражении огнем или подавлении помехами любого или любых из объектов.

$$\text{Э}_{\text{ССГВ}}^{\text{пр.с}} = 1 - \sum_{i=1}^{m} \mathrm{B}_{\text{ОС}_i}^{\text{выв}}, \quad (8)$$

где: $\text{Э}_{\text{ССГВ}}^{\text{пр.с}}$ — эффективность системы связи группировки войск по пропускной способности;

$i = 1,2,\ldots,m$ — количество выводимых из строя объектов связи;

$\mathrm{B}_{\text{ОС}_i}^{\text{выв}}$ — важность i-го выведенного из строя объекта связи.

Предполагается, что объекты связи, выведенные из строя за время выполнения системой связи рассматриваемой боевой задачи, восстановлению не подлежат.

Расчет важности объектов связи производится в три этапа:

на *первом* этапе определяется важность линий и путей связи в каждом из направлений рассматриваемой системы связи пункта управления;

на *втором* этапе определяется важность объектов связи, входя-

щих в рассматриваемую систему связи пункта управления;

на *третьем* этапе определяется важность объектов связи, обслуживающих системы связи различных пунктов управления, входящих в систему рассматриваемой группировки войск.

После ранжирования объектов связи в каждой из организуемых систем связи пунктов управления определяется относительная важность объектов системы связи группировки войск ($В_{ОС_{ССГВ}}$):

$$В_{ОС_{ССГВ}} = \sum_j^n \sum_i^m В_{ОС_{ijССПУ}},$$

где: $i = 1, 2,\ldots,m$ — количество направлений связи, организуемых от i-го пункта управления;

$j = 1, 2,\ldots,n$ — количество систем связи пунктов управления в составе системы связи группировки войск.

Предлагаемые для практического применения методики оценки эффективности позволяют быстро и просто получить объективное представление о последствиях принимаемых решений на построение и использование систем военной связи применительно к прогнозируемым условиям обстановки. Объективность результатов оценки эффективности рассматриваемой системы связи будет зависеть в основном от достоверности используемых исходных данных и ошибок, допускаемых при проведении расчетов.

$$В^{отн}_{ОС_{ССГВ}} = В_{ОС_{ССГВ}} \left(\sum_{i=1}^{m} В_{ОС_{ССГВ_i}}\right)^{-1}_{ССПУ},$$

где $i = 1, 2,\ldots,m$ — количество объектов связи в составе системы связи группировки войск.

Универсальность и простота представленного методологического подхода, положенного в основу рассмотренной методики оценки эффективности системы связи, предназначенной для количественного обоснования решений по организации связи, предоставляют большие возможности по его использованию в других методиках, обеспечивающих решение широкого круга задач боевой подготовки и боевого применения войск связи.

ПРИМЕЧАНИЯ

[1] *Ермишян А.Г.* Теоретические основы построения систем военной связи в объединениях и соединениях: учебник. Ч. 1. Методологические основы построения организационно-технических систем военной связи. СПб.: ВАС, 2005. 740 с.

[2] Теоретические основы построения систем военной связи в объединениях и соединениях: учебник / под общ. ред. Ю.А. Пирогова. Ч. 2. СПб.: ВАС, 2007. 610 с.

[3] *Воробьев И.Г.* Управление трафиком в транспортной сети связи специального назначения на основе сбора информации об интенсивности информационных потоков и их прогнозировании / Труды XIII ВНПК РАРАН «Актуальные проблемы защиты и безопасности». Изд. в 6 т. Т. 1: ВиВТ. СПб.: НПО СМ, 2010. С. 66—69.

Применение перспективных средств РЭБ для противодействия системам авиационной радиотехнической разведки при прикрытии мобильных комплексов ПВО

Генерал-майор В.В. МИХАЙЛОВ

Подполковник В.И. СЕРГЕЕВ,
доктор технических наук

Майор Д.А. ФИЛИН

АННОТАЦИЯ

Для повышения эффективности прикрытия мобильных комплексов противовоздушной обороны (ПВО) от авиационных многопозиционных систем радиотехнической разведки предложены пути применения перспективных наземных станций помех по радиоподавлению разведывательной аппаратуры.

ABSTRACT

To improve the efficiency of covering mobile air defense (AD) units against aviation multiposition systems of radio-engineering reconnaissance the paper proposes ways of using advanced ground-based jamming stations for radio suppression of reconnaissance equipment.

КЛЮЧЕВЫЕ СЛОВА

Авиационная радиотехническая разведка, станции помех.

KEYWORDS

Aviation radio-engineering reconnaissance, interference station.

ПРИМЕНЕНИЕ ПЕРСПЕКТИВНЫХ СРЕДСТВ РЭБ ДЛЯ ПРОТИВОДЕЙСТВИЯ СИСТЕМАМ АВИАЦИОННОЙ РАДИОТЕХНИЧЕСКОЙ РАЗВЕДКИ

ОПЫТ военных конфликтов последних десятилетий показывает, что характерной особенностью боевых действий авиации стран НАТО является приоритетное уничтожение наземных средств ПВО.

Используемый сейчас подход по подавлению наземной ПВО, реализуемый в рамках оперативной концепции *Destruction of Enemy Air Defense* (*DEAD*), предполагает широкое применение средств воздушной высокоточной (ВТ) радиотехнической разведки (РТР) для вскрытия позиций мобильных зенитно-ракетных комплексов (ЗРК) путем точного измерения координат их РЛС с последующим нанесением по ним удара. При этом в условиях боевой обстановки, когда требуется вскрыть работающие средства ПВО за достаточно короткое время и оперативно передать информацию о них носителям оружия, предпочтение отдается многопозиционным системам воздушной ВТ РТР, обеспечивающим более высокие точность и оперативность выдачи целеуказания[1].

Одним из путей защиты подразделений ПВО на боевых позициях является использование средств РЭБ. На сегодняшний день проблема противодействия системам наведения противорадиолокационных ракет (ПРР) и управляемых авиабомб (УАБ) методами и средствами РЭБ проработана достаточно глубоко и позволяет в ряде типовых ситуаций реализовывать эффективное прикрытие защищаемых объектов. Это обеспечивается в основном за счет использования отвлекающих источников и средств радиоподавления радионавигационных приемников ПРР и УАБ.

Однако гарантированная защита ЗРК может быть обеспечена лишь при комплексном подходе, который подразумевает противодействие как бортовым средствам радионавигации и системам наведения ПРР и УАБ, так и системам воздушной ВТ РТР.

В настоящее время существующая и перспективная техника РЭБ имеет ограниченные возможности по борьбе с указанными системами, а теоретические вопросы противодействия им в известной литературе рассмотрены мало, что определяет актуальность поиска возможных путей противодействия воздушной ВТ РТР противника.

Основные принципы пространственно-распределенной РТР были разработаны в США еще в начале 1970-х годов и реализованы в ходе создания воздушной системы РТР *Guardrail Common Sensor* на базе самолетов *RC-12*, которая до сих пор используется для обеспечения данными разведки командования армейского корпуса и более высоких звеньев управления сухопутных войск США. Высокая точность определения координат радиоизлучающих РЭС достигалась благодаря использованию комбинации нескольких методов их определения, в первую очередь разностно-дальномерного и угломерного[2].

Серьезным недостатком системы *Guardrail Common Sensor*, затрудняющим ее использование в рамках оперативной концепции *DEAD*, является невозможность определения координат излучающих РЭС противника и выдача по ним целеуказания в масштабе времени, близком к реальному. Из-за отсутствия на борту *RC-12* операторов по обработке добываемой информации все полученные данные вначале сбрасываются на наземные пункты обработки. Лишь затем обработанные данные поступают в центр

управления воздушными операциями или передаются в виде целеуказания непосредственно на ударные самолеты.

Для парирования указанного недостатка в ВВС США с 90-х годов прошлого века ведутся работы по созданию пространственно-распределенной системы ВТ РТР на базе самолета дальнего радиолокационного обнаружения и управления *E-3C*. Оснащение данного самолета станцией РТР *AN/AYR-1*, аппаратурой системы передачи данных «Джитидс», а также бортовой ЭВМ с расширенными вычислительными возможностями позволило придать ему функции пункта обработки информации системы ВТ РТР, где в качестве ведомого самолета (приемного пункта разведки) может использоваться любой летательный аппарат, оснащенный комплектом аппаратуры РТР, всенаправленной приемной антенной и аппаратурой системы передачи данных с повышенной пропускной способностью (например, самолет-разведчик *RC-135 Rivet Joint*, самолет РЭБ *EA-18G* «*Growler*» или беспилотный летательный аппарат типа *RQ-4 Global Hawk*).

Типовой состав пространственно-распределенных систем ВТ РТР на базе самолета *E-3C* включает не менее двух-трех приемных пунктов (ПП) — летательных аппаратов с аппаратурой РТР и средствами информационного обмена и пункт обработки информации (ПОИ). Ведомые носители аппаратуры РТР в зависимости от тактических условий размещаются на расстоянии от единиц до десятков километров друг от друга. Примерный вариант размещения такой системы приведен на рисунке 1.

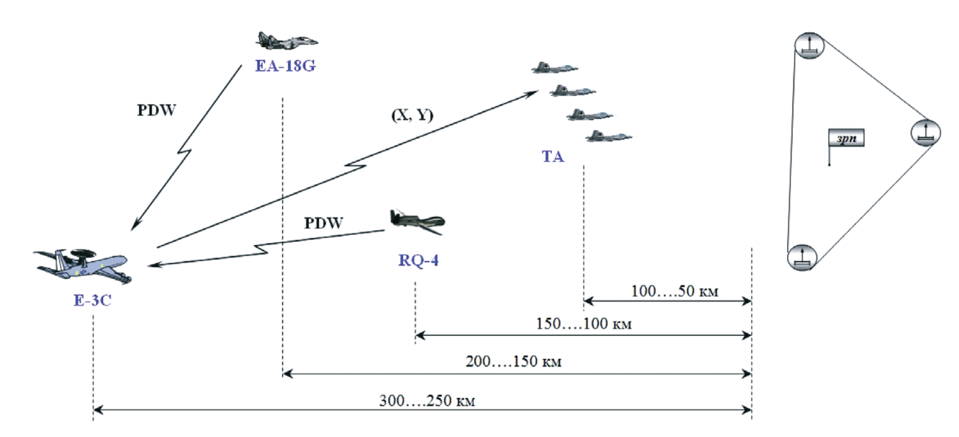


Рис. 1. Вариант схемы построения авиационной системы высокоточной РТР противника

При ведении РТР в составе системы осуществляется синхронный обзор по диапазонам рабочих частот, обнаружение импульсных сигналов РЛС, оценивание их параметров. Полученные данные записываются в поимпульсные дескрипторы (*Pulse Descriptor Word — PDW*). В заданные интервалы времени совокупность дескрипторов совместно с координатами и параметрами движения летательного аппарата — носителя аппаратуры РТР передается на ПОИ.

На ПОИ осуществляется отождествление дескрипторов, принятых аппаратурой РТР различных носителей, по результатам которого осуществляется текущая оценка координат РЛС. Координаты, полученные при последовательных наблюдениях, сглаживаются в соответствии с текущими ошибками их оценивания.

Возможные направления использования средств РЭБ для противодействия системам ВТ РТР могут быть связаны с созданием:

• помех радиолиниям передачи данных между ведомыми ПП системы РТР и ПОИ системы;

• помех бортовой радионавигационной аппаратуре ПП;

• помех приемникам РТР, приводящих к увеличению ошибок оценивания времени прихода импульсов и неправильному отождествлению сигналов разных ПП с последующим ошибочным определением координат РЛС.

Первое и второе направления представляют собой самостоятельные и широко известные научно-технические задачи подавления радиосвязи и радионавигации. Третье направление является новым и рассматривается детально.

К ключевым особенностям функционирования системы ВТ РТР, существенным с точки зрения создания помех разведывательным приемникам, следует отнести:

• функционирование системы разведки в пассивном режиме;

• использование прецизионного способа оценивания времени прихода зондирующего сигнала РЛС по переднему фронту импульса[3,4];

• широкие (десятки — сотни МГц) полосы пропускания приемных трактов аппаратуры РТР.

Перечисленные особенности обусловливают следующий ряд достаточно существенных проблемных вопросов, возникающих при обосновании способов радиоподавления приемной аппаратуры системы ВТ РТР.

1. Сложность локализации с высокой (не хуже десятков метров) точностью приемных пунктов системы РТР штатными средствами обнаружения подразделений РЭБ. В реальных условиях задача идентификации ПП системы требует своего решения на основе анализа радиолокационной и радиотехнической информации о наблюдаемых воздушных объектах. Элементы воздушной многопозиционной системы РТР должны обладать совокупностью следующих траекторных и сигнальных признаков: наличие 3—4 объектов, разнесенных друг от друга на десятки километров; траектория их полета примерно совпадает с линией боевого соприкосновения (или государственной границей); между объектами осуществляется интенсивный обмен данными.

2. Необходимость информационно-технического сопряжения станций помех (СП) системе РТР с защищаемыми РЛС для информационного обеспечения реализуемых способов радиоподавления.

3. Необходимость использования многолучевых средств с независимым формированием помех в каждом луче.

Преодоление приведенных требований с использованием существующего парка техники РЭБ[5,6] практически нереализуемо, что до настоящего времени ограничивало пути противодействия многопозиционной воздушной РТР организационно-техническими мерами, направленными на имитацию излучений РЛС с использованием ложных источников в точках стояния этих источников и повышение скрытности излучений защищаемых РЛС.

Разрабатываемые и перспективные СП имеют значительно более высокие возможности, позволяющие потенциально парировать приведенные выше ограничения. Из их числа необходимо отметить следующие[7]:

• возможность реализации любых видов помеховых сигналов, в том числе воспроизводящих потоки импульсов прикрываемых РЛС;

• возможность многолучевого излучения с одновременным формиро-

ванием независимых потоков помеховых сигналов в каждом луче;

- использование в некоторых образцах перспективной техники РЭБ радиолокационных каналов для отслеживания текущего положения ПП системы разведки.

Анализ перечисленных возможностей в соотношении с уязвимыми местами авиационных многопозиционных систем РТР позволил определить следующие возможные способы радиоподавления их приемной аппаратуры.

Способ радиоподавления на основе маскирования излучений РЛС

Суть способа заключается в скрытии сигналов прикрываемой РЛС на входе приемной аппаратуры системы РТР путем создания маскирующих шумовых помех. Пространственная схема реализации рассматриваемого способа приведена на рисунке 2.

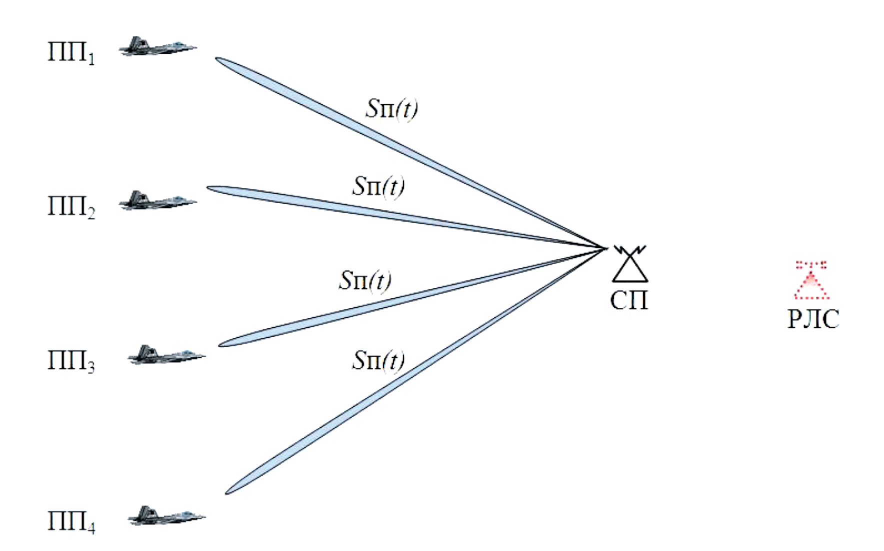


Рис. 2. Пространственная схема реализации способа радиоподавления на основе маскирования излучений РЛС

Необходимое для реализации способа число СП — одна-две, а в состав информационного обеспечения входят данные о координатах прикрываемой РЛС, о текущем местоположении ПП системы РТР, а также частотное расписание функционирования РЛС. Последний пункт предполагает обеспечение СП информацией о расписании смены рабочих частот РЛС и ее сигнальных характеристик с периодичностью не реже 8—10 раз в секунду.

Из достоинств способа следует отметить возможность его реализации принятыми на снабжение СП генераторного типа[8,9], а из недостатков: дефицит энергопотенциала СП, жесткие требования к выбору позиции СП для обеспечения электромагнитной совместимости с прикрываемой РЛС и демаскирование собственных позиций СП, которые будут достаточно оперативно вскрыты авиационной многопозиционной системой РТР угломерным методом.

Последний недостаток довольно существенен, что обусловливает низкую конфликтную устойчивость способа прикрытия РЛС.

Способ радиоподавления на основе имитации РЛС в заданных точках

Целью реализации способа является формирование на экране оператора ПОИ системы РТР ложных источников (ЛИ) за счет излучения в направлении на каждый *i*-ый ПП сигналов $Sп_i(t)$, аналогичных сигналам защищаемой РЛС, с управляемыми задержками в каждом луче. Пространственная схема реализации способа с наблюдаемыми системой РТР объектами при его реализации приведена на рисунке 3.

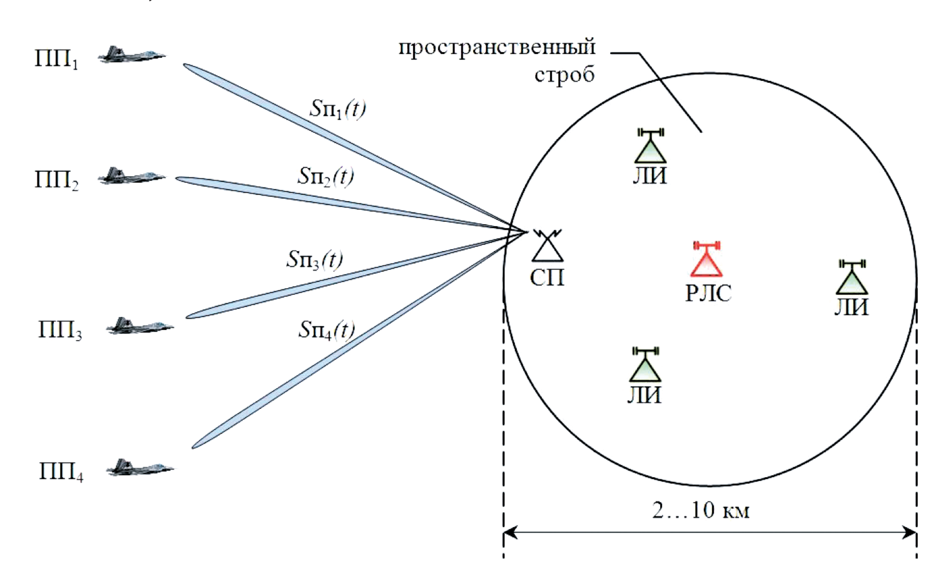


Рис. 3. Пространственная схема реализации способа

Величина задержки излучения помехи в направлении на *i*-й ПП вычисляется таким образом, чтобы обработка совокупности сигналов $Sп_i(t)$ на пункте обработки информации системы РТР привела бы к появлению ложных координат в заданных точках.

Реализация способа возможна с использованием одной многолучевой СП и требует информации о типе и координатах защищаемой РЛС, а также о текущем местоположении ПП системы разведки.

Из достоинств способа следует отметить отсутствие необходимости информационного сопряжения с защищаемой РЛС и возможность имитации нескольких РЛС с использованием одной СП в режиме временного разделения. Из недостатков необходимо выделить наличие на экране оператора ПОИ среди ложных истинной отметки РЛС (рис. 3).

Во избежание вскрытия истинных координат СП системой РТР угломерным методом позиции СП и прикрываемой РЛС должны находиться в пределах одного пространствен-

Сложность локализации с высокой (не хуже десятков метров) точностью приемных пунктов системы РТР является проблемой при обосновании способов радиоподавления приемной аппаратуры. В реальных условиях задача идентификации ПП системы требует своего решения на основе анализа радиолокационной и радиотехнической информации о наблюдаемых воздушных объектах.

ного строба аппаратуры измерения угловых координат на ПП, что проиллюстрировано на рисунке 3 (выделено серым). Данное требование распространяется и на следующий способ радиоподавления.

Способ радиоподавления на основе упреждающей имитации фронта импульса РЛС

Способ радиоподавления на основе упреждающей имитации фронта импульса РЛС

Суть предлагаемого способа заключается во внесении ошибок в результаты измерения времени прихода импульсов РЛС на приемные пункты системы РТР за счет излучения упреждающих по времени прихода на ПП помеховых импульсов.

Пространственная схема выполнения способа аналогична предыдущим способам, а основная его идея заключается в том, что на каждый импульс РЛС в направлении каждого (или части) приемного пункта системы РТР излучаются помеховые импульсы. Моменты их излучения рассчитаны таким образом, чтобы импульс помехи появлялся на ПП со случайным временным упреждением относительно импульса РЛС, перекрываясь с ним по времени. Несущие частоты импульсов помех выбираются так, чтобы импульсы прикрываемой РЛС и СП не разрешались в приемных устройствах системы РТР.

Это исключит возможность системы РТР правильно оценить время прихода импульса РЛС, исключив тем самым правильное измерение координат РЛС разностно-дальномерным методом.

Из достоинств способа следует отметить пониженные требования к знанию текущего положения приемных пунктов системы РТР, а из недостатков — необходимость технического сопряжения с прикрываемыми РЛС.

Таким образом, показано, что задача прикрытия РЛС систем ПВО от воздушной высокоточной системы РТР противника представляется решаемой, но весьма сложной в организационно-техническом плане. Рассмотрены возможные пути решения этой задачи методами и средствами РЭБ, а также связанные с ними способы радиоподавления на основе использования перспективных наземных станций помех.

ПРИМЕЧАНИЯ

[1] *Старков В.М., Шушков А.В.* Высокая точность и большая мощность // Воздушно-космическая оборона. 2009. № 1 (44). С. 30—32.

[2] Там же.

[3] *Козлов С.В., Усков А.В.* Оценивание координат источника радиоизлучения, размещенного на воздушном объекте, в системах радиомониторинга с использованием группового учета и декоррелирующих преобразований ошибок определения координат приемных пунктов // Радиотехника. 2014. № 9. С. 41—45.

[4] *Мельников Ю.П.* Воздушная радиотехническая разведка (методы оценки эффективности). М.: Радиотехника, 2005. С. 304.

[5] *Ласточкин Ю.И.* Радиоэлектронная борьба. Основные этапы развития 1904—2014. Рязань: ООО «Печатный дом», 2014. С. 488.

[6] Радиоэлектронные технологии России: альманах / под ред. И.Г. Насенкова. М.: Ассоциация «Лига содействия оборонным предприятиям», 2012. С. 484.

[7] Там же.

[8] Там же.

[9] *Ласточкин Ю.И.* Радиоэлектронная борьба. Основные этапы развития 1904—2014. С. 488.

О правовом регулировании применения искусственного интеллекта в военной сфере

Полковник юстиции Е.А. ГЛУХОВ,
кандидат юридических наук

АННОТАЦИЯ

Несмотря на широкое внедрение в военной сфере средств автоматизации и искусственного интеллекта, их правовое обоснование в настоящее время практически отсутствует. Выявляются пробелы в правовом регулировании применения искусственного интеллекта в военных целях, вносятся предложения о разработке нормативных правовых актов.

ABSTRACT

Despite the increasing introduction of automation and artificial intelligence assets in the military sphere, their legal justification is virtually nonexistent at the moment. The paper highlights the gaps in the legal regulation of artificial intelligence use for military purposes, offering suggestions as to normative legal acts development.

КЛЮЧЕВЫЕ СЛОВА

Искусственный интеллект, военный робот, автоматическое оружие, военное управление, принятие решений, средства ведения войны, военное право.

KEYWORDS

Artificial intelligence, military robot, automatic weapons, military control, decision taking, warfare assets, military law.

ПРИМЕНЕНИЕ средств вооруженной борьбы с использованием искусственного интеллекта (ИИ) по масштабам и эффективности можно смело сравнить с революцией в военном деле, которая произошла с появлением ракетно-ядерного оружия. На вооружение ряда стран уже приняты системы с элементами ИИ, начиная с беспилотных летательных аппаратов, роботов-часовых и заканчивая системами обработки сложной информации.

Так, например, в июле 2016 года стало известно о компьютерной программе ВВС США под названием *ALPHA*. Она позволяет не только управлять полетом истребителя, но и побеждать в воздушном поединке опытного военного летчика в виртуальном бою. В ходе других испытаний нейросетевые алгоритмы успешно провели не только ближний маневренный воздушный бой, но и выявляли противника с помощью радаров, а потом поражали его ракетами[1].

В сухопутных войсках также активно внедряются технологии искусственного интеллекта. Например, в начале 2019 года командование армии США инициировало программу разработки виртуального помощника для экипажей танков и боевых машин, которые призваны повысить эффективность применения техники и вооружения в условиях современного боя. Виртуальный помощник *ATLAS* будет обнаруживать цели, которые люди не сразу замети-

ли, оценивать их опасность, а также наводить на цель орудие. При этом система *ATLAS* будет не только обрабатывать данные с собственных датчиков и устройств боевой машины, но и получать данные извне, что увеличит вероятность обнаружения целей. Как заявлено в технической документации системы, она позволит обнаруживать, идентифицировать и поражать цели как минимум в 3 раза быстрее, чем сейчас делает человек»[2].

В военно-морских силах США используют боевую информационно-управляющую систему *Aegis*, позволяющую принимать и обрабатывать информацию с датчиков кораблей и летательных аппаратов и выдавать целеуказание на ракетные пусковые установки[3]. Решение на поражение противника принимает человек (оператор), но можно настроить систему таким образом, чтобы цели поражались в автоматическом режиме без участия человека. Более того, согласно предполагаемой американской стратегии, летальное боевое оружие устанавливается на вспомогательные корабли ВМФ, а решение на их применение принимается дистанционно. Другими словами, на самих кораблях, где установлены боевые ракеты, отсутствует команда, призванная обслуживать и осуществлять пуск ракет[4].

Министерство обороны США осуществляет около 600 проектов с применением искусственного интеллекта, а инвестиции в них выросли с 600 млн долл. в 2016 году до 2,5 млрд долл. в 2021 финансовом году[5]. По взглядам высшего военного руководства США, одной из ключевых задач на современном этапе военного строительства является интеграция технологий искусственного интеллекта в существующие и новые образцы военной техники[6].

Председатель компартии Китая также неоднократно отмечал важность внедрения ИИ во все сферы жизнедеятельности государства, в том числе и в оборонную отрасль[7]. НОАК ежегодно тратит более 1,6 млрд долл. на системы с поддержкой ИИ, не считая засекреченных разработок — говорится в исследовании американских ученых[8].

Таким образом, в настоящее время наблюдается очередной виток гонки вооружений, но теперь уже в информационно-технологической сфере. Более 40 стран, в том числе США, Россия, Великобритания, Франция, Китай, Израиль, Южная Корея, разрабатывают роботов, способных воевать без человеческого участия[9]. Планируется, что к 2030 году доля боевых технических средств с ИИ составит 52 % от количества экипажных боевых машин и 30 % — от общего состава боевых машин. При этом, по оценкам американских военных специалистов, боевые возможности подразделений нового типа возрастут в 2—2,5 раза[10].

В России также ведутся разработки по оснащению электронными системами управления современного вооружения и техники. Некоторые образцы «умных машин» уже поступили в российскую армию. Например, в 2021 году в ходе учений успешно поражали цели такие российские наземные «беспилотники», как «Уран-9», оснащенный пушкой, пулеметом, противотанковыми ракетами и огнеметом, а также система «Нерехта». Управление такими машинами осуществлялось в режиме реального времени операторами, находившимися на удалении 1,5 км. В 2022 году планируется проведение опытного учения с использованием боевой робототехники, по результатам которого будет принято решение об оптимальном количестве поставки такой боевой техники в войска[11].

На актуальность внедрения в новые образцы вооружения технологий

ИИ обращал внимание Президент Российской Федерации В.В. Путин: «…технологии искусственного интеллекта должны обеспечить качественный прорыв в повышении боевых характеристик оружия, должны активнее применяться в системах управления, средствах связи и передачи данных, а также высокоточных ракетных комплексах. Не менее важно внедрение технологий искусственного интеллекта при создании перспективной робототехники с повышенной степенью автономности, в обеспечении управления беспилотниками, а также глубоководными аппаратами. Все эти приоритеты и задачи должны быть в полной мере отражены в государственной программе вооружения до 2033 года»[12]. Выступая на коллегии Минобороны России за 2020 год, Президент России рекомендовал «в ходе боевой учебы более активно осваивать, «обкатывать» вооружения и технику с элементами искусственного интеллекта, в том числе — роботизированные комплексы, автоматизированные системы управления. Такое оружие в разы повышает потенциал частей и соединений и в ближайшем будущем станет во многом определять исход боя»[13].

Не случайно, что на развитие ИИ в России до 2024 года планируется выделить 244 млрд руб.[14] В 2020 году Минобороны России уже заказало разработку системы искусственного интеллекта для использования в военных целях. Стоимость контракта, который должен быть исполнен до 10 ноября 2022 года, составила 387,8 млн руб. При этом в 2020 году на эти исследования планировалось выделить более 115 млн руб., в 2021 году — свыше 152 млн руб., а в 2022-м — 120 млн руб.[15]

Поэтому вполне естественным фактом было появление в структуре Минобороны России нового органа — Главного управления инновационного развития, одной из основных функций которого является внедрение высокотехнологичной продукции военного и специального назначения в интересах обороны[16].

Центральные СМИ сообщают, что не позднее 2035 года в Российской армии произойдет переход к созданию полностью автономных беспилотников и групп военной техники. Внедрение систем автоматического распознавания целей нового поколения не только повысит эффективность разведывательных летательных аппаратов, но и резко снизит их потенциальные боевые потери[17].

Все вышеизложенные примеры свидетельствуют об актуальности и неотложности более пристального научного рассмотрения вопросов разработки и внедрения новых систем вооружения и техники, где применяются технологии ИИ. Тем более правовая регламентация данного процесса, как обычно, отстает от фактических достижений. Да, законодательство РФ более-менее регламентирует гражданские отношения, связанные с производством и продажей вооружения и военной техники. Еще детальнее государство описывает порядок применения ручного огнестрельного оружия. Но вот применение умных машин, использование ИИ в военных целях регламентировано крайне слабо, тем более — открытыми (несекретными), доступными для всеобщего ознакомления нормативными правовыми актами. В настоящее время в Российской Федерации отсутствует специальное законодательное регулирование, учитывающее специфику применения технологий искусственного интеллекта и робототехники[18]. Между тем указанная правовая проблема в такой опасной, но важной для обороны и целостности государства в сфере обороны вряд ли оправдана

Выступая на коллегии Минобороны России за 2020 год, Президент России рекомендовал «в ходе боевой учебы более активно осваивать, «обкатывать» вооружения и технику с элементами искусственного интеллекта, в том числе — роботизированные комплексы, автоматизированные системы управления. Такое оружие в разы повышает потенциал частей и соединений и в ближайшем будущем станет во многом определять исход боя».

и может привести к критическим последствиям.

Можно уверенно утверждать, что технический прогресс в очередной раз обогнал правовое регулирование общественных отношений в области создания технических новинок. Кстати, подобная правовая неопределенность существует и в отношении допуска на дороги общего пользования беспилотных транспортных средств. В обоих случаях речь идет не просто о применении нового прибора или машины, а об эксплуатации устройств, способных самостоятельно, т. е. без участия человека получать информацию, анализировать ее, принимать решения и реализовывать их. Таким образом, самостоятельные действия подобного рода устройств (как под контролем оператора, так и без его контроля) будут порождать правовые последствия для отдельных лиц.

Хочется обратить особое внимание на весьма важный момент в сфере рассматриваемых отношений. Системы с использованием ИИ нельзя отождествлять просто с роботами или автоматизированными системами управления, которые действуют строго по заданной программе. На опасность подмены понятий указывает, в частности, профессор В.М. Буренок, говоря, что искусственный интеллект — это компьютерный феномен, хотя и не обладающий интеллектуальными способностями человека, но уже и не ограниченный в своих решениях неким жестким алгоритмом и способный выйти в своих действиях за рамки этого алгоритма.

Автоматизация процессов управления с помощью компьютеров не является тождественной работе системы ИИ. В первом случае речь идет о вычислительных машинах, оснащенных совокупностью алгоритмов обработки информации, которая затем используется как система исходных данных для решения задач с помощью формализованных методов. Основные отличия интеллектуализации по отношению к автоматизации — это реализация способности компьютера принимать решения в условиях значительной неопределенности, на основе разнородной и неполной информации, часто меняющихся ситуаций, в том числе за пределами заложенных алгоритмов программы. Можно сказать, что ИИ — это способность компьютера принимать решения в разнообразных и быстро меняющихся ситуациях аналогично человеку[19].

Ключевой момент здесь — самостоятельность действий технического устройства, выраженная в возможности анализировать, принимать решения и реализовывать их, не согласуясь с человеком, будь то оператор, владелец или программист. Устройство, наделенное ИИ, гораздо более самостоятельное, нежели просто технический прибор, пусть даже работающий по сложной программе. А самое важное в данном аспекте — это самостоятельность такой компьютерной системы, ее способность делать выводы и при-

нимать решения в зависимости от результатов анализа данных и даже обладание ею творческими функциями[20]. При применении военных роботов с ИИ оператор всего лишь задает конечную цель, а не конкретные шаги для ее достижения.

Более того, ИИ обладает еще одним важным качеством — он способен к самообучению и адаптации к различным условиям, т. е. к изменению алгоритмов своих действий или даже структуры с целью достижения оптимального состояния при изменении внешних условий. Такое техническое устройство под управлением искусственного интеллекта способно на основе предыдущего опыта и новой информации самостоятельно изменять и совершенствовать изначально заложенное в нее программное обеспечение, осуществлять самопрограммирование (изменять и дополнять заложенную в нее программу), а значит, и решать задачи, которые не были предусмотрены при создании данного устройства изначально. Поэтому так крайне важно исходя из указанных характеристик совершенствовать систему законодательства о применении систем с ИИ.

В российском законодательстве понятийно-терминологический аппарат сферы регулирования искусственного интеллекта заложен Указом Президента Российской Федерации от 10 октября 2019 года № 490 «О развитии искусственного интеллекта в Российской Федерации», утвердившим «Национальную стратегию развития искусственного интеллекта на период до 2030 года»[21]. В указанном документе дается следующее определение искусственного интеллекта — это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач ***результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека.***

Таким образом, на уровне нормативного правового акта РФ закреплено положение о самообучении и саморазвитии компьютерной программы. Следовательно, заложенная в техническое средство (например, в робота или в сервер) такого рода компьютерная программа через некоторое время изменится, будет отличаться от первоначальной программы; причем данное изменение будет происходить без участия сторонних лиц.

Вышеуказанная Стратегия предусматривает поэтапное создание нормативно-правовой базы, способной обеспечить формирование и функционирование комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием технологий ИИ. К 2024 году должны быть созданы необходимые правовые условия для решения задач и реализации мер, предусмотренных Стратегией, а к 2030 году — гибкая система нормативно-правового регулирования в области искусственного интеллекта, в том числе гарантирующая безопасность населения и направленная на стимулирование развития технологий ИИ.

Вместе с тем следует признать, что в упомянутой Стратегии речь идет о разработке системы законодательства прежде всего в сфере гражданского права. Другими словами, декларируется развитие законодательства относительно исключительных прав на продукцию с элементами ИИ, правил оборота такой продукции, ответственности за возможный вред в результате ее функционирования и субъектах, которые должны будут данный вред компенсировать. Учеными-юристами вполне серьезно обсуждается возможность наделе-

ния ИИ определенной правосубъектностью в будущем, заключения им сделок и возложения гражданско-правовой ответственности за его действия[22].

Однако в отечественной юридической науке практически не разработаны сами правовые аспекты применения искусственным интеллектом военной силы (и использования искусственного интеллекта военными структурами); в законодательстве отсутствуют соответствующие нормы права, устанавливающие рамки для использования ИИ на военной службе. Тем более не определены критерии отнесения сотрудников военных организаций к субъектам уголовной ответственности при причинении вреда военными роботами.

Существуют лишь общие нормы о применении вооружения и военной техники, а также общие положения об ответственности за причинение вреда. Однако существующие нормы права не учитывают специфики наличия ИИ, не учитывают специфики воинских правоотношений. Кроме того, отсутствие норм права о порядке использования технических средств с ИИ означает и то, что они не могут быть нарушены, а без нарушения норм права невозможно и само правонарушение, а также юридическая ответственность. В Конституции Российской Федерации закреплен принцип, согласно которому никто не может нести ответственность за деяние, не признававшееся правонарушением в момент его совершения (ст. 54).

Проблема видится в том, что до конца не ясны границы и сам предмет правового регулирования относительно применения военных систем искусственного интеллекта. Законодательные акты, регулирующие данные правоотношения, не созданы, крайне скупо представлено регулирование данного вопроса и в военных ведомствах. Указанная проблема констатируется в Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года[23]. При этом, как было указано выше, сами технические средства с элементами ИИ уже существуют.

В зарубежной юридической литературе уже несколько десятков лет достаточно последовательно формируется так называемое «робоправо» или «право роботов» как самостоятельная предметная область исследования. Рассматриваются прежде всего проблемы ответственности, правосубъектности, контролируемости систем ИИ, проблемы авторского и патентного права и многие другие[24,25].

Однако, во-первых, вышеуказанные исследования иностранных ученых нельзя применить к российской действительности по причине различия законодательства в разных странах, несовпадения уровней технического и экономического развития, менталитета населения и принципов государственной политики. Российской науке еще предстоит проработка данного вопроса. Как указано в Программе фундаментальных научных исследований в России на долгосрочный период (2021—2030 годы)[26], «в центре внимания будут оставаться вопросы… правового и информационного пространства. Необходимы междисциплинарные исследования в сфере правового регулирования вопросов развития робототехники, уточнения правового статуса ИИ».

А во-вторых, законодательство в военной сфере имеет существенную специфику. В отличие от, например, беспилотного автомобиля *Tesla*, функцией которого является перемещение людей и грузов с наименьшим причинением вреда[27], роботизированные комплексы, применяемые в интересах обороны страны, одной из главных функций имеют имен-

но причинение вреда живой силе и технике противника, иной заданной цели. Либо они опосредованно связаны с вышеуказанной функцией причинения вреда. Вред, причиняемый ими, возникает, как правило, не случайно, не в результате форс-мажора, а целенаправленно в результате их применения по назначению. В этих целях системы ИИ обладают возможностями применения оружия, разведывательной деятельности, анализом информации (в том числе персональных данных), разрушения объектов, причинения вреда жизни и здоровью людей и т. п. Следовательно, в военной сфере системы, наделенные ИИ, потенциально гораздо более опасны.

Международное гуманитарное право уже много лет разрабатывает нормативную базу, касающуюся запрета использования ряда средств и методов ведения войны. Согласно Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие[28], право воюющих сторон выбирать методы или средства ведения войны не является неограниченным. Запрещается применение в вооруженных конфликтах оружия, снарядов и веществ и методов ведения войны, которые могут нанести чрезмерные повреждения или принести излишние страдания[29].

Так, под запрет попадают следующие средства войны:

• взрывчатые и зажигательные пули; пули, легко разворачивающиеся или сплющивающиеся в человеческом теле; удушливые, ядовитые или другие подобные газы и бактериологические средства;

• бактериологическое (биологическое) и токсичное оружие, конкретные виды обычного оружия (необнаруживаемые осколки в человеческом теле, некоторые виды мин, зажигательное оружие и оружие массового уничтожения — в отношении гражданского населения), средства воздействия на природную среду, химическое оружие;

• ослепляющее лазерное оружие.

Существуют лишь общие нормы о применении вооружения и военной техники, а также общие положения об ответственности за причинение вреда. Однако существующие нормы права не учитывают специфики наличия ИИ, не учитывают специфики воинских правоотношений. Кроме того, отсутствие норм права о порядке использования технических средств с ИИ означает и то, что они не могут быть нарушены, а без нарушения норм права невозможно и само правонарушение, а также юридическая ответственность.

Как видим, в международных конвенциях прямо не предусмотрен запрет на применение систем с ИИ, да и сами указанные международные акты были приняты еще до внедрения в жизнь такого рода технических систем. Но здесь уместно сделать важную оговорку: не вся военная техника с элементами ИИ является собственно оружием. Многие виды военной техники, включая авто- и воздушные беспилотники, созданы не как оружие, а как вспомогательные и обслуживающие системы. ИИ может существовать и в компьютерных сетях, выполняя интеллектуальную функцию, помогая принимать решения командованию либо участвуя в кибервойне с противником. В этом случае не требуется ни шасси, ни огнестрельного оружия, ни иного технического устройства.

В современных реалиях грань между оружием и иным техничес-

ким изделием военного назначения размывается. Например, нанести вред противнику можно не только выстрелив в него из огнестрельного оружия, но и путем вывода из строя его систем управления, либо переключением управления на себя, поражения систем жизнеобеспечения посредством компьютерных вирусов, DDoS-атак, воздействуя звуком, светом, магнитным излучением, распространением дезинформации, отдачи ложных команд и т. п.

Например, голосовой искусственный интеллект может точно смоделировать голос любого человека. Представьте, что случится, когда в условиях войны или боя по радиосвязи или телефонной связи (в том числе ЗАС) вы получите команды, отдаваемые «голосом командира» (на самом деле — отдаваемых противником)? Их выполнение подчиненными приведет к дезорганизации управления и поражению в битве[30]? Ответ очевиден: противнику будет нанесен существенный вред, вполне возможно, погибнут люди, войска окажутся в невыгодном положении.

Ведение современных войн не предусматривает длительных и кровопролитных сражений, но вместе с тем продолжают совершенствоваться средства, в результате применения которых противнику будет нанесен невосполнимый вред именно в критическом для него месте. Это может быть финансовая или энергетическая сфера, деятельность органов управления и тому подобное.

В то же время на вооружении многих армий стоят и военные роботы, имеющие в качестве составляющего элемента боевое оружие, которое предназначено поражать живую силу противника. Да, любое оружие производится для того, чтобы предостерегать агрессора и при необходимости причинять ему вред. Поэтому свободное обращение оружия ограничено законодательством, а использование его по назначению должно осуществляться строго на основе закона по установленной процедуре.

Системы ИИ могут и не быть оружием. Например, их применяют для навигации, связи, разведки, наблюдения и рекогносцировки, разминирования, логистики, обслуживания вооружения и техники, информационной войны, радиоэлектронной борьбы, обучения и контроля обучения, автоматического распознавания целей, подготовки управленческих решений, программного выведения из строя электрических и телекоммуникационных сетей противника. Развитие систем вооружения и ускорения темпа боевых действий заставляет военное командование максимально автоматизировать управление войсками, ибо человеческий мозг уступает компьютеру в скорости обработки такого количества информации.

Но и не будучи оружием (в обычном смысле данного слова), системы ИИ в армии все равно предназначены для повышения боеспособности своих войск и нанесения урона противнику. Так, беспилотные аппараты могут осуществлять таран и не имея огнестрельного оружия, т. е. все равно способны наносить вред, в том числе убивать человека. Ситуацию еще более осложняет тот факт, что вред они могут приносить без непосредственной команды человека. Следует отметить, что ни в международном праве, ни в российском законодательстве не закреплено требование обязательного участия человека при реализации роботом его смертоносного действия (т. е. «нажатия на курок» или одобрения решения).

К настоящему времени сложились три разновидности военных роботов: с заложенной изначально жесткой программой действий, управляемые человеком-оператором, с искусствен-

ным интеллектом. В западной классификации это выглядит так:

- «человек-в-системе-управления» (human-in-the-loop) — роботы способны самостоятельно обнаруживать цели и осуществлять их селекцию, однако решение об их уничтожении (или на иные действия) принимает только человек-оператор;
- «человек-над-системой-управления» (human-on-the-loop) — к этой категории относятся системы, способные самостоятельно обнаруживать и выбирать цели, а также принимать решения в отношении них, но человек-оператор, выполняющий роль наблюдателя, в любой момент может вмешаться и скорректировать или заблокировать данное решение;
- «человек-вне-системы-управления» (human-out-of-the-loop) — к этой категории отнесены роботы, способные обнаруживать, выбирать и уничтожать цели самостоятельно, без человеческого вмешательства[31].

Полностью автономная система способна принимать решения и совершать действия в условиях отсутствия контроля со стороны человека. Этот уровень автономии следует отличать от систем, которые либо «взаимодействуют» с человеком, либо зависят от некоторой формы контроля с его стороны[32].

Таким образом, следует констатировать, что современные автономные системы вооружения могут действовать полностью самостоятельно, без вмешательства оператора: от поиска цели до принятия решения и лишения человека жизни, даже если он не в военной форме. И такие случаи уже зафиксированы. Так, в 2020 году турецкие дроны *Kargu* 2, используя «тактику роя», выследили и атаковали повстанцев в Ливии. Причем сделали они это самостоятельно, без участия человека[33]. Другой случай — в ноябре 2020 года в Иране был убит ученый-ядерщик М. Фахризаде, руководитель центра исследований при минобороны Ирана. Выстрелы были произведены из пулемета под управлением компьютерной системы, без участия человека[34].

В России летом 2021 года были внесены изменения в Федеральный закон «Об оружии». В частности, уточнялось, что оружие является источником повышенной опасности[35]. И хотя под регулирование данного закона подпадает лишь небольшая часть оружия, используемого Вооруженными Силами РФ и иными военными ведомствами[36], законодатель четко определил вектор правового регулирования в рассматриваемой сфере правоотношений. Ведь если к источникам повышенной опасности законодатель отнес боевое ручное стрелковое и холодное оружие, то тем более таким источником являются гораздо более смертоносные танки, пушки, огнеметы, торпеды и т. д.

Как указывается в юридической литературе, источнику повышенной опасности военного назначения присущи определенные специфические признаки: повышенная вредоносность, масштабность причинения вреда. Такого рода военные объекты способны причинить вред, несмотря на самый полный контроль за ними со стороны человека[37].

По общему правилу, чем выше риск для нарушения прав человека либо причинения вреда, тем более строгим должно быть правовое регулирование в данной сфере отношений. Соответственно сферы, связанные с особенно высокими рисками, такие как оборона страны, правоохранительная деятельность, применение оружия либо источников повышенной опасности, должны быть урегулированы наиболее детально. Однако в реальности все обстоит не так. Ученые признают казус отсутствия даже международных договоров об использовании новых технологий ведения военных действий, хотя их развитие и возмож-

ность применения в вооруженных конфликтах не должны происходить в правовом вакууме[38].

В этом плане хочется поддержать Илона Маска в его высказывании, что искусственный интеллект намного опаснее, чем ядерное оружие. Искусственный интеллект — это тот редкий случай, когда нужно проявлять инициативу в регулировании, а не пытаться реагировать на его деятельность постфактум[39].

Конечно, разработка алгоритмов, реализуемых в составе программного обеспечения робототехнических систем, осуществляется по техническим заданиям и требованиям ГОСТ. Но все же нельзя подменять правовое регулирование, обязательное для всех субъектов и обеспечиваемое принуждением государства, регулированием техническим, определяющим лишь желательные параметры производимых объектов.

В рамках настоящей публикации, конечно же, невозможно дать качественную юридическую оценку всем аспектам применения систем ИИ в военной сфере. Следует уже сегодня начать вырабатывать концепцию применения систем ИИ в военной сфере, в частности, рассмотреть следующие проблемные вопросы:

Определить те направления воинской деятельности, в которых допустимо применение систем с ИИ. В частности, требует правовой регламентации вопрос: «Вправе ли системы ИИ добывать, обрабатывать и хранить информацию о персональных данных граждан[40], иную охраняемую законом информацию, сведения, содержащие государственную тайну?». Также уже сегодня необходимо нормативно задать перечень ситуаций, когда управление в части принятия значимых решений должен принять на себя человек.

Определить те виды оружия и вооружения, которые не могут оснащаться системами ИИ, так как спусковой крючок такого смертоносного оружия может нажимать только человек.

Ведение современных войн не предусматривает длительных и кровопролитных сражений, но вместе с тем продолжают совершенствоваться средства, в результате применения которых противнику будет нанесен невосполнимый вред именно в критическом для него месте. Это может быть финансовая или энергетическая сфера, деятельность органов управления и тому подобное.

Регламентировать права, обязанности и ответственность воинских должностных лиц, которые применяют системы с ИИ с тем, чтобы предупредить совершение ими преступлений, запрещенных нормами международного гуманитарного права. Иначе есть вероятность, что такое смертоносное и умное оружие станет просто средством достижения преступных целей, средством причинения смерти на расстоянии.

Определить, когда ИИ вправе принимать решения самостоятельно, не дожидаясь одобрения оператора, например, в случаях необходимости защиты от нападения противника (решение об уничтожении ракеты или дрона, приближающегося к пункту управления). Требует уточнения и вопрос о принятии ИИ самостоятельных решений в наступательных операциях (т. е. применения оружия не для защиты), а также принятия решений, касающихся применения кибероружия.

Уточнить баланс полномочий и ответственности между человеком и системой ИИ в случае, когда искусственный интеллект осуществляет подготовку решения для дальнейше-

го его одобрения человеком. В условиях скоротечности современных военных действий и существенного опережения счетно-аналитических способностей компьютера по сравнению с человеком любое промедление в принятии решений может повлечь поражение. В то же время нельзя сводить роль человека к нажатию любой кнопки, которую рекомендует ИИ, т. е. к роли собаки Павлова, но только с оружием. Желательно определить те параметры, при наличии которых оператор вправе без наличия негативных юридических последствий для себя не согласиться с предложенным ИИ вариантом решения.

Требует правовой регламентации порядок осуществления контроля за деятельностью ИИ и предоставления объективной информации владельцу, контролирующим и надзирающим органам.

Определить ситуации, когда системы с ИИ должны прекратить выполнение программы уничтожения людей (поднятый противником белый флаг или поднятые вверх руки, классификация цели как некомбатанта, раненый военнослужащий и пр.).

Определить субъектов, которые вправе владеть и использовать технологии ИИ военного назначения. Недопустимо, чтобы такого рода военные системы могли попасть к террористам или преступникам.

Важнейшей проблемой регулирования ИИ и робототехники является вопрос ответственности: кто отвечает за действия робота, особенно военного? Поэтому необходимо четко и ясно регламентировать баланс ответственности государства, военного командования, производителя систем с ИИ перед третьими лицами за вред, причиненный в ходе использования военных роботов. В качестве самостоятельных направлений законодательного регулирования требуется уточнить ответственность за вред, причиненный не оружием, а кибератаками, а также ответственность за вред, причиненный в результате технического сбоя в работе систем ИИ, т. е. без наличия причинно-следственной связи с действиями оператора. Вполне возможно, необходимо будет корректировать законодательство об обязательном страховании гражданской ответственности применительно к эксплуатации систем с ИИ[41].

Подлежит отдельному рассмотрению вопрос, кто должен нести ответственность за действия ИИ, обладающего способностью к самообучению? Ведь ИИ способен самостоятельно принять решение о совершении противоправных действий или бездействия, которые повлекут наступление вреда. Если алгоритм работы программы модифицируемый, то разработчик не может отвечать за применение робототехнической системой после модификации того, что он разработал, а человек, эксплуатирующий его, не может полноценно управлять и контролировать систему с неизвестными ему правилами поведения[42].

Безусловно, автономная система в вычислении чисел, поиске большого объема данных и их сортировке, быстром реагировании на срочные задания, способности одновременно выполнять несколько задач, в том числе сложных, превосходит способности человека. Однако только он — человек, способен размышлять, проявлять милосердие, применять имеющийся опыт к новым возникающим задачам, принимать осмысленные решения и нести за них юридическую ответственность[43].

Вывод: государство, которое победит в гонке по созданию ИИ, получит критическое и, возможно, неоспоримое военное преимущество, однако данный процесс должен происходить обязательно строго в правовом поле.

ПРИМЕЧАНИЯ

[1] Flightglobal. URL: https://www.flightglobal.com/fixed-wing/darpa-tests-artificial-intelligent-dogfighting-in-two-versus-one-simulations/142993.article (дата обращения: 30.01.2022).

[2] Breakingdefense. URL: https://breakingdefense.com/2019/03/atlas-killer-robot-no-virtual-crewman-yes/? (дата обращения: 30.01.2022).

[3] Aegis BMD, MDA. URL: http://www.mda.mil/system/Aegis bmd.html (дата обращения: 30.01.2022).

[4] The National Interest. URL: https://nationalinterest.org/blog/reboot/spread-out-and-networked-how-navy-plans-fight-and-win-future-wars-183803 (дата обращения: 10.02.2022).

[5] Коммерсантъ. 2021. 15 сентября.

[6] Department of Defense. Electro-magnetic Spectrum Superiority Strategy. October 2020. URL: https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/electromagnetic_spectrum_superiority_strategy.pdf (дата обращения: 30.01.2022).

[7] *Струкова П.Э.* Искусственный интеллект в Китае: современное состояние отрасли и тенденции развития // Вестник Санкт-Петербургского университета. Востоковедение и африканистика. 2020. Т. 12. Вып. 4. С. 588—606.

[8] *Харпер Д.* Китай сравнялся с Пентагоном по уровню ИИ // Журнал Национальной обороны США (National defense magazine) 2022. 6 января.

[9] *Фаличев О., Галанин Ю.* Железные контрактники // Военно-промышленный курьер. 2018. 2 октября.

[10] *Буренок В.М., Ивлев А.А., Корчак В.Ю.* Развитие военных технологий XXI века: проблемы планирование, реализация. Тверь: Издательство ООО «КУПОЛ», 2009. 624 с.

[11] Интервью Главнокомандующего Сухопутными войсками ВС РФ генерала армии О. Салюкова // Красная звезда. 2021. 1 октября.

[12] Выступление В.В. Путина на совещании с руководством Минобороны России и предприятий ОПК 3 ноября 2021 г. // Официальный сайт Президента России http://kremlin.ru/events/president/news/67061 (дата обращения: 30.01.2022).

[13] Официальный сайт Президента России. URL: http://kremlin.ru/events/president/news/64684 (дата обращения: 30.01.2022).

[14] *Литовкин Д.* Бездушная армия. Зачем Минобороны меняет солдат на роботов // https://tass.ru/opinions/11452767 (дата обращения: 30.01.2022).

[15] Аналитическое агентство TAdviser. URL: https://www.tadviser.ru/index.php/Компания:Управление_Минобороны_РФ_по_развитию_искусственного_интеллекта#cite_note-0 (дата обращения: 10.02.2022).

[16] Официальный сайт Минобороны России URL: https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=11376@egOrganization (дата обращения: 30.01.2022).

[17] *Птичкин С.* Искусственный интеллект все чаще помогает военным // Российская газета. 2020. 23 августа.

[18] Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // СЗ РФ. 2020. № 35. Ст. 5593.

[19] *Буренок В.М.* Искусственный интеллект в военном противостоянии будущего // Военная Мысль. 2021. № 4. С. 106—112.

[20] *Аверкин А.Н., Гаазе-Рапопорт М.Г., Поспелов Д.А.* Толковый словарь по искусственному интеллекту. М.: Радио и связь. 1992. 256 с.

[21] Национальная стратегия развития искусственного интеллекта на период до 2030 года. Утв. Указом Президента РФ от 10.10.2019 № 490 // СЗ РФ. 2019. № 41. Ст. 5700.

[22] См, например, *Лаптев В.А.* Понятие искусственного интеллекта и юридическая ответственность за его работу // Право. Журнал Высшей школы экономики. 2019. № 2. С. 79—102.

[23] Концепция развития регулирования отношений в сфере технологий искус-

ственного интеллекта и робототехники до 2024 года. Утв. Распоряжением Правительства РФ от 19.08.2020 № 2129-р // СЗ РФ. 2020. № 35. Ст. 5593.

[24] Hellström Thomas On the moral responsibility of military robots // Ethics and Information Technology. 2013. Vol. 15. P. 99—107.

[25] *Palmerini E., Bertolini A., Battaglia F.* et al. RoboLaw: Towards a European framework for robotics regulation // Robotics and Autonomous Systems. 2016. Vol. 86. P. 78—85.

[26] Утв. Распоряжением Правительства РФ от 31.12.2020 № 3684-р // СЗ РФ. 2021. № 3. Ст. 609.

[27] В феврале 2022 года американская компания TuSimple, чей грузовик первым в мире совершил полноценный автономный 700-километровый рейс без человека в кабине или удаленного оператора, заявила, что нашла первого коммерческого клиента для такого рода рейсов. URL: www.tusimple.com

[28] Заключена в г. Женеве 10.10.1980 // Ведомости ВС СССР. 1984. № 3. Ст. 50.

[29] Ст. 23 IV Гаагской конвенции о законах и обычаях сухопутной войны от 18.10.1907 // Международное гуманитарное право в документах. МНИМП. М., 1996. С. 575—587.

[30] *Захарцев С.И. и др.* Искусственный интеллект в механизме развития человеческой цивилизации / С.И. Захарцев, Н.Д. Литвинов, В.П. Сальников, В.С. Чернявский // Юридическая наука: история и современность. 2021. № 4. С. 47—73.

[31] Cook A. Taming killer robots: Giving meaning to the «Meaningful human control»: Standard for lethal autonomous weapon systems – Air University Press. Maxwell Air Force Base, Alabama, 2019.

[32] *Холиков И.В.* Некоторые проблемные вопросы международно-правовой регламентации использования беспилотных морских систем в военных целях // Военное право. 2019. № 6. С. 276—282.

[33] *Грищенко Н.* Беспилотник впервые выследил и атаковал человека без участия оператора // Российская газета. 2021. 31 мая.

[34] *Bergman R., Fassihi F.* The Scientist and the A.I.-Assisted, Remote-Control Killing Machine // The New York Times. 2021. September 19.

[35] Федеральный закон от 28.06.2021 № 231-ФЗ «О внесении изменений в Федеральный закон “Об оружии” и отдельные законодательные акты Российской Федерации» // СЗ РФ. 2021. № 27 (ч. I). Ст. 5059.

[36] См. Постановление Правительства РФ от 15.10.1997 № 1314 (ред. от 15.07.2021) «Об утверждении Правил оборота боевого ручного стрелкового и иного оружия, боеприпасов и патронов к нему, а также холодного оружия в государственных военизированных организациях» // СЗ РФ. 1997. № 42. Ст. 4790.

[37] *Лейба В.Н.* Ответственность воинской части по обязательствам, возникающим вследствие причинения вреда: дис. ... канд. юрид. наук. М.: ВПА, 1973. С. 71—72.

[38] *Рыльская М.А.* Кибервойна: новый взгляд на проблему семантической и правовой идентификации // Военное право. 2020. № 1. С. 243—250.

[39] Elon Musk Says Artificial Intelligence Is the ‘Greatest Risk We Face as a Civilization’ // Fortune. 2017. July 15.

[40] В настоящее время согласно ст. 3, 7 и 9 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 02.07.2021) «О персональных данных» получение, обработка и распространение персональных данных, в том числе фотоизображений, возможно только с согласия самого человека.

[41] Президент России В.В.Путин поручил Правительству РФ проработать данный вопрос (см. Перечень поручений по итогам конференции «Путешествие в мир искусственного интеллекта», утв. Президентом РФ 16.12.2021 № Пр-2371). URL: http://kremlin.ru

[42] *Тиханычев О.В.* Автономная робототехника: о проблеме контроля модифицируемых алгоритмов // Вопросы безопасности. 2020. № 2. С. 36—47.

[43] *Чернявский А.Г., Сибилева О.П.* Автономное высокоточное оружие как вызов международному гуманитарному праву // Военное право. 2020. № 4. С. 229—238.

Управление жизненным циклом образцов вооружения, военной и специальной техники с искусственным интеллектом

С.В. ГАРБУК,
кандидат технических наук

АННОТАЦИЯ

Рассмотрены особенности технологий искусственного интеллекта (ИИ) и впервые сформулирована взаимоувязанная система требований к разработке, созданию, эксплуатации и утилизации вооружения, военной и специальной техники (ВВСТ) с ИИ, показаны особенности распределения требований между функциональными системами и составными частями данных образцов, обоснованы общие принципы контроля их соответствия установленным требованиям и реагирования на выявленные несоответствия.

КЛЮЧЕВЫЕ СЛОВА

Управление жизненным циклом ВВСТ, процессы жизненного цикла ВВСТ, качество ВВСТ, искусственный интеллект, оборонные задачи искусственного интеллекта, стандартизация требований к системам искусственного интеллекта.

ABSTRACT

The paper looks at the specifics of artificial intelligence (AI) technologies and pioneers description of an interconnected system of requirements for the development, creation, operation and utilization of armaments, military and specialized equipment (AMSE) with AI, showing the specific features of requirements distribution between functional systems and constituents of the said items, and justifying the general principles of control over their correspondence to the set requirements and reaction to mismatches revealed.

KEYWORDS

Control over AMSE lifecycle, AMSE lifecycle processes, AMSE quality, artificial intelligence, defense tasks for artificial intelligence, standardizing requirements for artificial intelligence systems.

УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ ОБРАЗЦОВ ВООРУЖЕНИЯ, ВОЕННОЙ И СПЕЦИАЛЬНОЙ ТЕХНИКИ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

НА СОВРЕМЕННОМ этапе одним из наиболее перспективных направлений совершенствования вооружения, военной и специальной техники (ВВСТ) является применение технологий искусственного интеллекта (ИИ), позволяющих резко повысить эффективность решения задач сбора и обработки информации в различных образцах ВВСТ. При этом сдерживающим фактором полномасштабного внедрения ИИ в ВВСТ является недостаточная проработанность принципов управления жизненным циклом сложных технических систем, разработанных с использованием технологий ИИ.

Динамичное развитие современных отечественных вооружений, военной и специальной техники во многом основывается на принципах управления полным индустриальным (жизненным) циклом (ЖЦ) — от моделирования и проектирования до серийного выпуска изделий, обеспечения их эксплуатации и дальнейшей утилизации, заложенных Указом Президента Российской Федерации от 7 мая 2012 года № 603[1].

Общие проблемы создания системы управления ЖЦ ВВСТ на современном этапе рассмотрены в работах[2, 3, 4] и других. В частности, к таким проблемам относятся:

• слабая связанность работ на разных стадиях ЖЦ;

• отсутствие нормативных механизмов, предписывающих предприятиям промышленности проводить сервисное обслуживание и ремонт ВВСТ;

• неэффективность системы сбора информации о реальных показателях расхода ресурсов, надежности, готовности, затратах на каждом этапе жизненного цикла изделия;

• недостатки механизмов достоверного расчета стоимости каждого этапа жизненного цикла изделия;

• недостаточно развитые средства моделирования ЖЦ изделия, не позволяющие на стадии разработки прогнозировать его стоимостные и тактико-технические характеристики;

• незавершенность работ по переводу в цифровой вид проектной, научной, эксплуатационной и технической документации о существующих и разрабатываемых образцах ВВСТ;

• риски снятия с производства отдельных узлов и агрегатов ВВСТ.

При этом недостаточное внимание уделено вопросам управления полным ЖЦ ВВСТ, связанным с широкомасштабным использованием в образцах перспективных цифровых технологий, в частности технологий искусственного интеллекта (ИИ). Подобные проблемы непосредственно связаны с особенностями технологий ИИ, к которым можно отнести[5]:

• разработка систем ИИ предполагает обязательный этап обучения на прецедентах (обучающих наборах данных);

• алгоритмы обработки информации систем ИИ, обучаемых на прецедентах, могут принципиально не обладать свойствами интерпретируемости, объяснимости процесса вычислений и получаемых результатов;

• при аппаратно-программной реализации систем ИИ используются, как правило, специальные вычислительные средства (векторные, тензорные, нейроморфные процессоры и др.) и программные компоненты (программные библиотеки для машинного обучения и др.), оптимизированные для выполнения интел-

лектуальных алгоритмов обработки данных;

• значительная часть систем ИИ рассчитана на автоматизацию естественных интеллектуальных способностей человека;

• системы ИИ рассчитаны на работу с источниками слабо формализованных мультимодальных данных, отличающихся большими объемами, высокой изменчивостью и фрагментарностью;

• эффективность работ по созданию и применению прикладных систем ИИ принципиальным образом зависит от доступности обучающих и тестовых наборов данных разработчикам систем;

• обработка данных в системах ИИ может приводить к тому, что уровень конфиденциальности результатов обработки превышает уровень конфиденциальности исходных данных.

Особенности создания и функционирования системы управления ЖЦ в условиях применения технологий ИИ в образцах ВВСТ могут быть рассмотрены в разрезе общих задач управления ЖЦ, к которым в соответствии с ГОСТ Р 56135-2014[6] относятся:

а) задание взаимоувязанной системы требований к образцу ВВСТ, включающей требования к типовой конструкции ВВСТ и системе ее технической эксплуатации;

б) распределение принятых требований между функциональными системами (ФС) и составными частями (СЧ) комплекса (образца) в соответствии с принятыми схемами разукрупнения типовой конструкции;

в) контроль соответствия ВВСТ принятой системе требований на всех стадиях (этапах) ЖЦ;

г) разработка и контроль выполнения необходимых мероприятий в случае выявления несоответствия ВВСТ принятым требованиям.

Задание взаимоувязанной системы требований к образцу ВВСТ и системе ее технической эксплуатации

Перечисленные выше особенности интеллектуальных технологий обусловливают необходимость предъявления к образцам ВВСТ с ИИ дополнительных требований, выполнение которых гарантирует определенный уровень качества функционирования образцов с учетом особенностей и ограничений, присущих этим технологиям. Формирование таких специальных требований к ВВСТ может быть выполнено путем декомпозиции ЖЦ на отдельные процессы в соответствии с национальным стандартом ГОСТ Р 57193-2016[7]. Подобный подход является наиболее универсальным, так как не накладывает ограничений на последовательность реализации процессов на стадиях ЖЦ и, соответственно, инвариантен к используемой модели ЖЦ образца ВВСТ. В статье[8] проиллюстрирована возможность применения данного подхода на примере выявления основных задач стандартизации в области управления ЖЦ интеллектуальных систем информационной безопасности. В таблице 1 представлены специальные требования к ВВСТ с ИИ, соответствующие различным процессам ЖЦ, объединенным в четыре основные группы:

• процессы соглашения;

• процессы организационного обеспечения проекта;

• процессы технического управления;

• технические процессы.

Требования, приведенные в таблице 1, могут быть сгруппированы в следующие функциональные группы:

Таблица 1

Специальные требования к ВВСТ с ИИ при реализации различных процессов жизненного цикла

Группа процессов ЖЦ	Процесс ЖЦ	Вид специального требования к ВВСТ с ИИ
1. Процессы соглашения	1.1. Приобретение	при выборе поставщиков ВВСТ с ИИ в состав конкурентных процедур целесообразно включать требования по тестированию имеющихся у поставщиков прототипов ПО на подготовленных заказчиком наборах данных
	1.2. Поставка	при поставке ВВСТ с ИИ поставщику (разработчику) системы целесообразно включать в состав технической документации детальное описание условий, в которых был сформирован обучающий НД, с учётом заданного перечня существенных условий эксплуатации системы (существенных факторов)
2. Процессы организационного обеспечения проекта	2.1. Управление моделью ЖЦ	при формировании модели ЖЦ особо должна быть оговорена возможность дообучения ВВСТ с ИИ на стадии эксплуатации
	2.2. Управление инфраструктурой	для подтверждения качества ВВСТ с ИИ необходимы специальные средства испытаний алгоритмов ИИ, включая полигоны для физических и полунатурных испытаний, стенды для виртуальных испытаний алгоритмов
	2.3. Управление портфелем	для эффективного управления портфелем поставщика (разработчика) системы с ИИ необходимо устанавливать требования в области переноса обученных моделей ИИ на смежные прикладные задачи ИИ
	2.4. Управление человеческими ресурсами	а) в случае если в образце ВВСТ предусматривается автоматизация интеллектуальной деятельности человека с использованием технологий ИИ, для оценки качества ВВСТ с ИИ может понадобиться референтная группа квалифицированных операторов[9]; б) для эффективной разработки и применения ВВСТ с ИИ должны быть предусмотрены специальные образовательные программы в профильных вузах для подготовки специалистов по созданию и эксплуатации ВВСТ с ИИ
	2.5. Управление качеством	а) для типовых прикладных задач должны быть разработаны унифицированные перечни существенных функциональных характеристик алгоритмов ИИ и метрики, обеспечивающие оценку качества как степени соответствия значений функциональных характеристик требованиям[10]; б) если при эксплуатации ВВСТ с ИИ предусмотрено дообучение системы, то должны быть установлены процедуры выделения этапов для периодического контроля качества на стадии эксплуатации
	2.6. Управление знаниями	должны быть разработаны требования к процедурам повторного использования знаний, полученных в ходе обучения ВВСТ с ИИ, в том числе с использованием процедур «переноса обучения» (*transfer learning*)
3. Процессы технического управления	3.1. Планирование проекта	а) процесс планирования проекта в обязательном порядке должен предусматривать задачи по формированию и актуализации обучающих, тестовых и иных наборов данных, специфичных для конкретной прикладной задачи; б) если при эксплуатации ВВСТ с ИИ предусмотрено дообучение системы, то в плане должны быть предусмотрены этапы для периодического контроля качества на стадии эксплуатации

Продолжение таблицы 1

Группа процессов ЖЦ	Процесс ЖЦ	Вид специального требования к ВВСТ с ИИ
3. Процессы технического управления	3.2. Оценка и контроль проекта	—
	3.3. Управление решениями	на стадии проектирования ВВСТ с ИИ целесообразно предусмотреть возможность выбора типовой архитектуры системы ИИ, исходя из особенностей решаемой задачи
	3.4. Управление рисками	а) на этапе обучения и функционирования ВВСТ с ИИ должны учитываться риски, связанные с возможным неконтролируемым повышением уровня конфиденциальности обрабатываемых данных; б) на этапах верификации, валидации и функционирования ВВСТ с ИИ в обязательном порядке должны учитываться специфические риски систем ИИ, связанные с уязвимостью интеллектуальных алгоритмов к воздействию специфических атак на исходные данные, включая состязательные (*adversarial*) атаки
	3.5. Управление конфигурацией	должны быть предусмотрены процедуры документирования результатов дообучения ВВСТ с ИИ на стадии эксплуатации
	3.6. Управление информацией	а) должны быть предусмотрены требования к специфическим процедурам обработки информации, связанным с разметкой данных, необходимых для обучения, дообучения и тестирования ВВСТ с ИИ (далее — НД); б) должны быть разработаны специальные требования к качеству набора данных; в) должны быть разработаны требования к процедурам расширения (аугментации) НД; г) должны быть разработаны унифицированные форматы представления НД. Данная задача имеет место для любых информационных систем, но в случае систем ИИ приобретает особую актуальность вследствие размывания границ между стадиями сбора, хранения и предоставления доступа к данным; д) должны быть разработаны требования к обеспечению конфиденциальности НД, исключающих использование этих данных противником для повышения эффективности реализации угроз ИБ в отношении ВВСТ с ИИ; е) должны быть разработаны требования к методам и средствам гарантированной деклассификации НД, т. е. такого преобразования данных, при котором уровень их конфиденциальности необратимо становится достаточно низким и появляется возможность предоставления этих данных широкому кругу разработчиков ВВСТ с ИИ и другим заинтересованным лицам без рисков нарушения конфиденциальности по 3.6.д
	3.7. Измерения	а) должны быть разработаны требования к унифицированным процедурам измерения функциональных характеристик ВВСТ с ИИ, основанным на тестировании систем на представительных наборах данных; б) если некорректная работа ВВСТ с ИИ может привести к непосредственным угрозам безопасности третьих лиц, то должны быть предусмотрены унифицированные процедуры измерения (оценки) вероятности реализации таких угроз и тяжести последствий от их реализации
	3.8. Гарантии качества	а) унифицированные процедуры оценки функциональных характеристик (3.7.а), характеристик безопасности (3.7.б) и качества (2.5) ВВСТ с ИИ должны обеспечивать получение соответствующих оценок с заданными точностью и достоверностью в условиях действующих рисков (3.4) и применительно к планируемым условиям эксплуатации ВВСТ по 4.2; б) гарантии функциональной надежности и безопасности ВВСТ с ИИ должны обеспечиваться за счет выполнения требований по использованию при создании ВВСТ доверенных аппаратно-программных средств, преимущественно основанных на отечественных компонентах

Продолжение таблицы 1

Группа процессов ЖЦ	Процесс ЖЦ	Вид специального требования к ВВСТ с ИИ
4. Технические процессы	4.1. Анализ назначения	а) если технологии ИИ используются в ВВСТ для автоматизации интеллектуальной деятельности человека, то должны быть предусмотрены процедуры формализации соответствующей интеллектуальной прикладной задачи и определение функциональных возможностей 3.7. а и уровня безопасности 3.7.б референтной группы квалифицированных операторов (2.4.а); б) для ВВСТ с ИИ должны быть сформулированы функциональные требования (3.7.а) и требования по безопасности для третьих лиц (3.7.б). При этом могут учитываться возможности квалифицированных операторов 4.1.а по решению заданной прикладной задачи ИБ в ручном режиме
	4.2. Определение потребностей и требований заинтересованной стороны	а) для типовых прикладных задач должны быть разработаны перечни существенных функциональных характеристик алгоритмов ИИ (см. также 2.5.а); б) для предусмотренных условий эксплуатации ВВСТ с ИИ должны быть определены перечни внешних факторов, существенным образом влияющих на сложность решаемой прикладной задачи ИИ (перечень существенных условий эксплуатации ВВСТ); в) для предусмотренных условий эксплуатации должны быть определены диапазоны допустимых значений существенных условий эксплуатации (4.2.б), при которых должна сохраняться возможность применения ВВСТ с ИИ по назначению (область применения системы, *domain*) с гарантией по 3.8
	4.3. Определение системных требований	должен быть предусмотрен анализ объекта автоматизации (образца ВВСТ с ИИ), результатом которого будет являться обоснование технических требований к используемым алгоритмам ИИ (по возможности, без ограничений на способ реализации алгоритма), исходя из ожидаемых тактико-технических характеристик образца. Для такого анализа может быть использован подход, основанный на использовании трехуровневой иерархической модели объекта автоматизации, описанный в статье
	4.4. Определение архитектуры	определение архитектуры ВВСТ с ИИ в части реализации интеллектуальных алгоритмов обработки данных должно осуществляться с учетом требований по использованию доверенных (преимущественно отечественных) аппаратно-программных компонентов
	4.5. Определение проекта	—
	4.6. Системный анализ	должны быть предусмотрены процедуры, обеспечивающие выбор рационального компромисса между объяснимостью (понятностью, *transparency, explainability*) интеллектуальных алгоритмов ВВСТ с ИИ и качеством системы (по 2.4 и 2.5)
	4.7. Реализация	реализация ВВСТ с ИИ должна осуществляться с учетом требований по использованию доверенных (преимущественно отечественных) аппаратно-программных компонентов
	4.8. Комплексирование	—

Продолжение таблицы 1

Группа процессов ЖЦ	Процесс ЖЦ	Вид специального требования к ВВСТ с ИИ
4. Технические процессы	4.9. Верификация	а) должны быть разработаны требования к унифицированным методикам измерения существенных функциональных характеристик по 3.7.а и 4.2.а и методикам оценки рисков для третьих лиц по 3.7.б; б) при необходимости должны быть разработаны фрагменты тестовых наборов данных, на которых должно осуществляться измерение характеристик 4.9.а, и/или описание тестовых ситуаций, в которых необходимо измерять характеристики 4.9.а. Фрагменты тестовых наборов данных и описания тестовых ситуаций должны обеспечивать формирование тестовых НД, обладающих представительностью с учетом предполагаемых условий эксплуатации 4.2; в) должна быть обеспечена конфиденциальность тестовых наборов данных, используемых для оценки соответствия ВВСТ с ИИ предъявляемым требованиям, исключающая снижение достоверности получаемых оценок, вызванное переобучением алгоритмов ИИ
	4.10. Передача	в том случае если разработчику алгоритмов ИИ недоступны в полном объеме обучающие НД (например, вследствие режимных соображений) и окончательное дообучение ВВСТ с ИИ планируется заказчиком самостоятельно на стадии эксплуатации, должны быть предусмотрены процедуры распределения ответственности за достижение и сохранение требуемых ТТХ между разработчиком и заказчиком образца ВВСТ с ИИ
	4.11. Валидация	должны быть разработаны унифицированные методики подтверждения возможности успешного решения соответствующих прикладных задач в условиях эксплуатации 4.2
	4.12. Функционирование	а) на стадии функционирования должны быть установлены требования к процедурам дообучения ВВСТ с ИИ, учитывающие требования по управлению качеством 2.5.б; б) должны быть предусмотрены процедуры непрерывного контроля уровня конфиденциальности обрабатываемых данных, исключающие реализацию рисков в соответствии с 3.4.а
	4.13. Сопровождение	—
	4.14. Изъятие и списание	должны быть установлены требования к процедурам оценки уровня конфиденциальности данных, накопленных (сформированных) в процессе функционирования системы. Данные процедуры должны исключать нарушение конфиденциальности информации при изъятии и списании ВВСТ с ИИ

первая — требования к составу и способам измерения существенных функциональных характеристик и характеристик безопасности ВВСТ с ИИ (1.1., 2.2., 2.5.а, 3.4.б, 3.7.а, 3.7.б, 3.8.а, 3.8.б, 4.1.б, 4.2.а, 4.3., 4.6., 4.9.а, 4.9.б, 4.9.в, 4.11.);

вторая — требования по формализации предусмотренных условий эксплуатации ВВСТ с ИИ (4.2.б, 4.2.в);

третья — требования по унификации и обеспечению качества наборов данных, необходимых для создания и оценки соответствия ВВСТ с ИИ (1.2., 3.1.а, 3.6.а, 3.6.б, 3.6.в, 3.6.г);

четвертая — требования по использованию доверенных аппаратно-программных средств, преимущественно реализованных на отечественных компонентах (3.3., 3.8.б, 4.4., 4.7.);

пятая — требования по управлению дообучением ВВСТ с ИИ на стадии эксплуатации (2.1., 2.5.б, 2.6., 3.1.б, 3.5., 4.10., 4.12.а);

шестая — требования в области обеспечения конфиденциальности данных при создании и применении ВВСТ с ИИ (3.4.а, 3.6.д, 3.6.е, 4.12.б, 4.14.);

седьмая — требования по обеспечению возможности масштабирования и тиражирования алгоритмов ИИ на смежные прикладные интеллектуальные задачи (2.3., 2.6.);

восьмая — требования по оценке функциональных возможностей квалифицированного человека-оператора, осуществляющего в ручном режиме решение прикладной задачи, на автоматизацию которой направлено применение алгоритмов ИИ в ВВСТ (2.4.а, 4.1.а);

девятая — требования в области подготовки кадров (2.4.б).

Анализ сформированных групп требований показывает, что наиболее представительная группа (устанавливающая требования к наибольшему количеству процессов ЖЦ) связана со специфическими показателями качества интеллектуальных алгоритмов: особенностями формирования перечней и способами измерения значимых характеристик, определяющих функциональные возможности и уровень безопасности ВВСТ с ИИ.

На сегодняшний день общие вопросы оценки качества интеллектуальных алгоритмов являются достаточно хорошо изученными. Так, например, на рисунке 1 представлена матрица ошибок (*Confusion Matrix*) для задачи бинарной классификации, в которой *TP* — количество объектов, правильно отнесенных к классу *Positive*, *TN* — количество объектов, правильно отнесенных к классу *Negative*, *FP* — количество объектов, ошибочно отнесенных к классу *Positive* (количество ошибок первого рода, «ложная тревога»), *FN* — количество объектов, ошибочно отнесенных к классу *Negative* (количество ошибок второго рода, «пропуск цели»). Также на рисунке 1 приведены выражения для расчета оценок вероятностей наиболее часто используемых показателей ошибок работы алгоритмов ИИ, основывающиеся на вышеперечисленных четырех базовых показателях качества[11]. В общем случае матрица ошибок является квадратной матрицей, в которой элемент $C_{r,s}$ в строке *r* и столбце *s* соответствует количеству случаев, в которых объект, принадлежащий классу или категории *r*, был отнесен классификатором к классу *s*.

Представленные на рисунке 1 показатели качества являются универсальными и могут быть использованы для характеристики качества алгоритмов ИИ, разработанных на основе различных методов и используемых для решения разных задач. В то же время при решении конкретных прикладных задач ИИ используются, как правило, частные показатели качества, специфичные для определенной предметной области.

Так, основными показателями качества технологий распознавания слитной речи, используемых, например, в системах радиоэлектронной разведки (в англоязычной литературе используется термин *SIGINT*, *Signals Intelligence*) и в голосовых интерфейсах для управления образцами ВВСТ, являются:

• процент правильно распознанных слов (*WRR, Word Recognition Rate*);

• процент неправильно распознанных слов (*WER, Word Error Rate*), учитывающий количество замененных, удаленных слов и вставленных слов;

• процент неправильно распознанных предложений/фраз (*SER, Sentence Error Rate*).

		true condition				
	total population	condition positive	condition negative	Prevalence $= \frac{\sum condition\ positive}{\sum total\ population}$	Accuracy (ACC) $= \frac{\sum TP + \sum TN}{\sum total\ population}$	
predicted condition	prediction positive	True Positive (TP) Power	False Positive (FP) Type I error	Positive Predictive Value (PPV), Precision, Relevance $= \frac{\sum TP}{\sum prediction\ positive}$	False Discovery Rate (FDR) $= \frac{\sum FP}{\sum prediction\ positive}$	
	prediction negative	False Negative (FN) Type II error	True Negative (TN)	False Omission Rate (FOR) $= \frac{\sum FN}{\sum prediction\ negative}$	Negative Predictive Value (NPV) Separation Ability $= \frac{\sum TN}{\sum prediction\ negative}$	
		True Positive Rate (TPR) Sensitivity, Recall, Probability of Detection $= \frac{\sum TP}{\sum condition\ positive}$	False Positive Rate (FPR) Fall-out, Probability False Alarm $= \frac{\sum TN}{\sum condition\ negative}$	Positive Likelihood Ration (LR+) $= \frac{TPR}{FPR}$	Diagnostic Odds Rate (DOR) $= \frac{LR+}{LR-}$	F_1 score $= \left(\frac{TPR^{-1} + PPV^{-1}}{2}\right)^{-1}$
		False Negative Rate (FNR) Miss Rate $= \frac{\sum FN}{\sum condition\ positive}$	True Negative Rate (TNR) Specificity, Selectivity $= \frac{\sum TN}{\sum condition\ negative}$	Negative Likelihood Ration (LR-) $= \frac{FNR}{TNR}$		

Рис. 1. Матрица ошибок, иллюстрирующая способы вычисления оценок вероятностей наиболее распространенных показателей ошибок алгоритмов ИИ[11]

В интеллектуальных системах биометрической идентификации, применяемых, например, для аутентификации и оценки психофизиологического состояния военнослужащих, применяются следующие специальные показатели качества[12]:

- вероятность отказа регистрации — доля выборки, для которой система не может закончить процесс регистрации вследствие непредоставления необходимых биометрических характеристик, непредоставления при регистрации биометрического образца удовлетворительного качества, неподтверждения схожести со своим заново созданным шаблоном в процессе регистрации;
- вероятность отказа сбора данных — доля попыток верификации или идентификации, для которых биометрическая система не может получить или отобрать образец удовлетворительного качества, включая попытки, при которых биометрическая характеристика не может быть представлена (например, вследствие временной болезни или раны), попытки, при которых не удается произвести сегментацию или извлечение необходимых признаков, попытки, при которых извлеченные признаки не подходят по порогу проверки качества;
- вероятность ложного несовпадения — доля образцов, полученных в результате попыток подлинного лица, которые ошибочно признаны несовпадающими с шаблоном той же биометрической характеристики данного пользователя, представившего образец (аналогично *FNR* на рис. 1, если событием считать предъявление биометрической характеристики подлинным лицом);
- вероятность ложного совпадения — доля образцов, полученных в результате пассивных попыток «самозванца», которые ошибочно признаны совпадающими с шаблонами другого пользователя (аналогично *FPR* на рис. 1).

На основе этих базовых характеристик вычисляются дополнительные частные характеристики для систем верификации, систем идентификации на открытом множестве и на закрытом множестве.

Специфический набор характеристик качества используется также и для оценки интеллектуальных поисковых систем, применяемых для сбора информации из открытых источников (*OSINT, Open Source Intelligence*). Так, для определения качества работы поисковой системы в начале списка результатов поиска используется показатель «Точность на уровне *n* документов» *(Precision (n))*, который определяется как количество релевантных документов среди первых *n* документов, деленное на *n*. Например, если система выдает не более 10 документов на первой странице, то *Precision (10)* отражает качество результатов системы, получаемых на первой странице.

Для количественного сравнения работы поисковых систем на разных уровнях полноты (*TPR, Recall* на рис. 1) используется одиннадцатиточечная интерполированная средняя точность (*Eleven-point Interpolated Average Precision*). Для вычисления этой величины по каждому поисковому запросу точность измеряется в 11 точках на уровнях полноты 0.0, 0.1, 0.2…0.9, 1.0 на кривой «полнота-точность». Для оценки качества полной выдачи поисковой системы применяется показатель средняя точность (*Average Precision*), которая усредняет точность при выдаче каждого из *K* релевантных документов.

Точность на уровне *i*-го релевантного документа *Prec_rel (i)* равна *Precision (pos(i))*, если релевантный документ находится в результатах запроса на позиции *pos(i)*. Если *i*-й релевантный документ не найден, то *Prec_rel (i) = 0*. Средняя точность для заданного запроса равна среднему значению величины *Prec_rel (i)* по всем *K* релевантным документам. Усреднение величины средней точности по всем запросам дает величину *MAP* (*Mean Average Precision*) — число, которое характеризует работу поисковой системы по совокупности запросов.

Таким образом, видно, что для различных прикладных задач ИИ перечни используемых показателей качества могут существенно разниться и при использовании технологий ИИ в составе образцов ВВСТ актуальной является задача унификации характеристик используемых интеллектуальных алгоритмов. Такая унификация подразумевает использование релевантного классификатора задач ИИ, в котором для каждого класса задач могут быть сформулированы единые перечни характеристик качества соответствующих алгоритмов.

Один из возможных вариантов такой классификации алгоритмов ИИ, основанный на аналогии искусственного и естественного интеллекта, представлен в работе[13]. В классификаторе выделены следующие шесть основных групп интеллектуальных задач и соответствующих им алгоритмов ИИ (рис. 2):

1) распознавание образов;

2) категорирование, построение моделей окружающих объектов и процессов;

3) поиск решений;

4) реализация физических воздействий на окружающую среду;

5) автономное движение и позиционирование в пространстве;

6) социальные коммуникации.

Важно, что в соответствии с предложенной классификацией для каждого класса может быть определен не только единый перечень показателей качества алгоритмов, но и единый перечень факторов, определяющих сложность решения соответствующих интеллектуальных задач (существенных условий эксплуатации). Это открывает возможности по унификации требований в рамках второй группы «Требования по формализации предусмотренных условий эксплуатации ВВСТ с ИИ», процессы

Рис. 2. Универсальные классы задач искусственного интеллекта

4.2.б и 4.2.в (табл. 1). Например, существенными факторами в задачах распознавания образов являются:

- информационные возможности сенсоров (чувствительность, пространственное, временное и радиометрическое разрешение, полоса захвата и др.);
- количество и вариативность классов распознавания;
- уровень полиморфизма объектов одного класса, в том числе связанного с изменением ракурса, реконфигурацией и т. п.;
- продолжительность характерного поведенческого цикла объекта распознавания;
- характеристики фона и/или среды распространения электромагнитных волн (ЭМВ), в том числе уровень пространственно-временной изменчивости фона и среды распространения ЭМВ;
- уровень возможных преднамеренных искажений характеристик распознавания объектов (маскировка и др.), в том числе с использованием состязательных атак.

Совокупность факторов, определяющих существенные условия эксплуатации системы ИИ, должна учитываться при обосновании соответствующих требований к образцу ВВСТ в целом: соответствие установленным требованиям должно выполняться в заданных условиях эксплуатации. При этом целесообразно разделять следующие виды существенных факторов[14]:

- контролируемые управляемые факторы, включенные в методику испытания (как независимые переменные);
- контролируемые неуправляемые факторы (постоянные в течение испытаний), являющиеся частью условий испытания;
- неконтролируемые факторы — случайные и независимые от испытания факторы;

Для различных прикладных задач ИИ перечни используемых показателей качества могут существенно разниться и при использовании технологий ИИ в составе образцов ВВСТ актуальной является задача унификации характеристик используемых интеллектуальных алгоритмов. Такая унификация подразумевает использование релевантного классификатора задач ИИ, в котором для каждого класса задач могут быть сформулированы единые перечни характеристик качества соответствующих алгоритмов.

• незначительные факторы, эффект от которых не будет учитываться.

Особенностью приведенного выше классификатора задач ИИ также является его универсальность в смысле возможности применения как в оборонной, так и в гражданской сфере. Такое метрологическое единство в области ИИ облегчает трансфер технологий из гражданских областей экономики и открывает дополнительные возможности по повышению эффективности внедрения технологий ИИ в ОПК.

Распределение принятых требований между функциональными системами и составными частями образца ВВСТ

Образец ВВСТ в подавляющем большинстве случаев представляет собой сложную техническую систему (аппаратно-программный или роботизированный комплекс), и технологии ИИ, воплощенные в виде соответствующих алгоритмов, играют в этой системе более или менее значительную, но всегда ограниченную роль. В этой связи важно обеспечить унифицированные подходы к выявлению и локализации в составе образца интеллектуальной технологической компоненты, к которой могут быть предъявлены требования в соответствии с изложенными выше принципами.

Наиболее адекватным представляется подход, основанный на трехуровневой иерархической модели образца ВВСТ, проиллюстрированной на рисунке 3. На верхнем уровне иерархии выявляются типовые объекты автоматизации (ТОА), в которых применяются технологии ИИ. Объекты представляют собой сложные технические (организационно-технические) системы, предназначенные для решения функционально целостной группы отраслевых задач. Так, например, в оборонной сфере к таким объектам относятся[15, 16]:

• системы поддержки принятия решений различного уровня (стратегического, оперативно-тактического, тактического);

• высокоавтоматизированные средства ВВСТ (авиационные, морские и сухопутные вооружения и военная техника, средства ПРО, ПВО);

• высокоточное оружие;

• автономные робототехнические комплексы (наземные, воздушные, морские, многосредные);

• системы связи и управления войсками, вооружением и военной техникой;

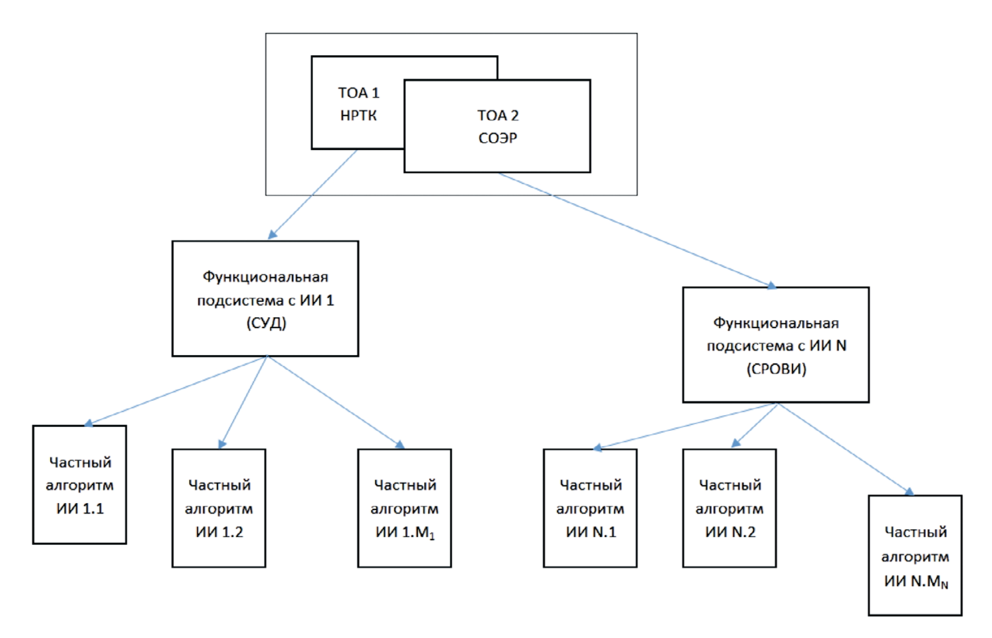
• системы разведывательно-информационного обеспечения;

• системы топогеодезического обеспечения;

• тактические средства поддержки военнослужащего (ландшафтная навигация, распознавание целей и решение задач «свой—чужой», контроль психофизиологического состояния военнослужащего, коммуникационное обеспечение, в том числе автоматический перевод иностранной речи и т. п.) и другие.

Перечни объектов автоматизации, в которых применяются технологии ИИ, могут устанавливаться в ведомственных организационно-распорядительных документах (в том числе годовом плане стандартизации военной продукции) и актуализируются по мере необходимости.

Технологии ИИ применяются в ТОА для решения различных задач, сформулированных в терминах военных потребителей. Например, применительно к наземным робототехническим комплексам могут быть выделены задачи автономной (без использования внешних радиона-



Примечание: НРТК — наземный робототехнический комплекс,
СОЭР — система оптико-электронной разведки,
СУД — система управления движением НРТК,
СРОВИ — система распознавания объектов военной инфраструктуры на аэрокосмических снимках.

Рис. 3. Структура объектов автоматизации, использующих технологий ИИ

вигационных полей) навигации, управления автономным движением, управления оружием и другие (рис.4). Предполагается, что для каждой из таких задач (функционально однородной группы задач) в составе объекта автоматизации предусмотрена отдельная функциональная подсистема (ФП), представляющая собой минимально достаточную совокупность персонала и технических средств автоматизации его деятельности[17], обеспечивающую решение соответствующих задач. Если в со-

Рис. 4. Функциональные подсистемы комплекса в составе командно-штабной машины (КШМ) и боевого робототехнического комплекса (БРТК)

ставе ФП используются технологии искусственного интеллекта, то она считается функциональной подсистемой с ИИ.

В каждой ФП с ИИ могут быть выделены один или несколько частных алгоритмов искусственного интеллекта, которые решают задачи распознавания образов, категорирования, восстановления регрессии и другие задачи, непосредственно относящиеся к классу задач ИИ. При этом важно отметить, что в состав ФП с ИИ могут входить также другие информационные системы и средства автоматизации, не использующие алгоритмы ИИ в своей работе.

Предлагаемая иерархическая структура объектов автоматизации позволяет сформировать целостную систему стандартов в области применения технологий ИИ для автоматизации ВВСТ. При этом в стандартах на уровне объекта автоматизации определяются специфические термины, связанные с применением интеллектуальных технологий, а также общие вопросы, относящиеся ко всем ФП с ИИ, включая:

- вопросы представления данных;
- особенности оборудования информационной инфраструктуры;
- общие требования к оформлению документов;
- перечень ФП, обработка данных в которых осуществляется с использованием алгоритмов ИИ, для данного ТОА.

Для каждой из ФП устанавливаются общие требования:

- перечень частных интеллектуальных алгоритмов в составе ФП с ИИ;
- описание эталонных архитектур, используемых для создания подсистем и частных алгоритмов (при наличии);
- требования к специальной инфраструктуре, обеспечивающей корректное функционирование соответствующей подсистемы (опционально). В случае необходимости могут разрабатываться другие стандарты, охватывающие отдельные аспекты общих требований к ФП с ИИ.

В свою очередь, для каждого из частных алгоритмов ИИ могут устанавливаться требования к способам испытаний, включающие:

1) общие требования:

- описание общих принципов испытания алгоритма;
- перечень существенных внешних условий эксплуатации системы ИИ, определяющих сложность решаемой интеллектуальной задачи и влияющих на результаты испытаний алгоритма ИИ;
- типовой состав входных данных;
- требования к испытательному оборудованию;
- правила оформления результатов испытаний;

2) показатели и критерии качества частного алгоритма ИИ:

- перечень показателей качества алгоритма;
- методики измерения каждого показателя качества алгоритма;
- правила свертки частных показателей качества к скалярной величине (интегральному показателю качества, опционально);
- критериальное правило для оценки качества алгоритма;

3) требования к тестовым наборам данных и сценариям испытания частного алгоритма ИИ:

- требования к представительности тестовых НД;
- фрагменты тестовых НД (базовые демонстрационные НД);
- правила формирования представительных тестовых НД (включая в случае необходимости описание представительной совокупности тестовых сценариев);
- принципы расширения (аугментации) тестовых НД.

Отметим, что в случае использования технологий ИИ в качестве основного способа испытаний алгоритма рассматривается его тестирование на представительном наборе размеченных данных, причем под представительностью понимается полнота и несмещенность выборки. Полнота набора данных обеспечивается с учетом описанных выше перечня существенных условий эксплуатации системы ИИ и перечня показателей качества алгоритма ИИ. Каждый фактор при этом может быть определен на своей шкале значений с учетом физического смысла фактора. Далее исходя из особенностей эксплуатации образца ВВСТ определяются законы распределения значений для каждого существенного фактора, учитывающие в том числе взаимные корреляционные связи факторов. В результате тестовая выборка может считаться несмещенной, если многомерный закон распределения существенных факторов для этой выборки с некоторой определенной погрешностью соответствует закону распределения факторов в процессе ожидаемых условий эксплуатации образца.

Предложенная структура специфических требований в области ИИ позволяет ограничиться определением роли и места алгоритмов ИИ в комплексном объекте ВВСТ с распределением частных интеллектуальных задач по отдельным ФП, описанием связанной с этим специальной терминологии и формированием детальных требований к методам испытаний используемых в системе интеллектуальных алгоритмов. При этом вопросы комплексных испытаний не затрагиваются, что позволяет избежать дублирования требований в области механических и термических испытаний, электромагнитной совместимости, эргономики и других вопросов, относящихся к объекту автоматизации в целом.

Контроль соответствия ВВСТ принятой системе требований на всех стадиях ЖЦ

Особенности контроля соответствия ВВСТ с ИИ принятой системе требований определяются моделью ЖЦ данного образца ВВСТ, устанавливающей последовательность и временные рамки процессов, необходимых для реализации ЖЦ, обеспечения и контроля характеристик задаваемых, проектируемых, изготавливаемых и эксплуатируемых образцов[18]. В зависимости от реализации того или иного процесса (см. табл. 1) на определенной стадии ЖЦ принимается решение о необходимости контроля соответствия требований, присущих процессам, реализуемым на соответствующей стадии.

В соответствии с ГОСТ Р 56135-2014 типовыми стадиями ЖЦ ВВСТ являются:

1) создание НТЗ;
2) формирование концепции образца (аванпроект);
3) разработка;
4) производство;
5) эксплуатация;
6) капитальный ремонт;
7) утилизация.

Таблица 2 иллюстрирует распределение специальных требований, принадлежащих различным группам, по стадиям ЖЦ ВВСТ с ИИ, соответствующее типовой модели жизненного цикла. Значения в ячейках таблицы соответствуют количеству видов требований определенной группы на заданной стадии ЖЦ. Стадия капитального ремонта (№ 6) исключена из таблицы, так как специальных требований

Таблица 2

Типовое распределение требований, принадлежащих различным группам, по стадиям ЖЦ образца ВВСТ с ИИ

№	Группа требований	Количество видов требований на стадиях ЖЦ ВВСТ с ИИ					
		1	2	3	4	5	7
1	Состав и способы измерения характеристик ВВСТ с ИИ	3	5	12	11	9	1
2	Формализация предусмотренных условий эксплуатации	0	1	2	0	2	0
3	Унификация и обеспечение качества наборов данных	2	1	4	5	3	0
4	Использование доверенных аппаратных средств	0	0	3	2	0	0
5	Управление дообучением ВВСТ с ИИ на стадии эксплуатации	0	1	1	1	6	1
6	Обеспечение конфиденциальности данных	0	0	0	3	5	5
7	Масштабирование и тиражирование алгоритмов ИИ	2	0	2	0	0	0
8	Оценка функциональных возможностей квалифицированного человека-оператора	0	1	1	1	2	0
9	Подготовка кадров	0	0	1	1	1	0
	Всего	7	9	26	24	28	7

к системам ИИ на этой стадии не предъявляется.

Анализ таблицы свидетельствует о том, что наибольшее количество требований приходится на стадию эксплуатации, а также на стадии разработки и производства ВВСТ с ИИ. На начальных стадиях (формирование научно-технического задела и обоснование концепции ВВСТ с ИИ) основное внимание уделяется обоснованию ТТХ систем, на стадии утилизации — обеспечению конфиденциальности данных, накопленных за время функционирования системы с ИИ.

Реагирование на выявленные несоответствия ВВСТ принятым требованиям

Реагирование на выявленные несоответствия ВВСТ с ИИ принятым требованиям осуществляется в целях изменения[19]:

- типовой конструкции и (или) системы технической эксплуатации ВВСТ для устранения несоответствий требованиям;
- принятой системы требований с учетом результатов конструктивной проработки ВВСТ и (или) накопления опыта их применения по назначению и ТО на стадии эксплуатации.

Выявление несоответствий установленным требованиям в области ИИ (табл. 2) может осуществляться на разных стадиях ЖЦ и при выполнении различных процессов. Реализация мер по реагированию на выявленные несоответствия

осуществляется субъектами управления ЖЦ ВВСТ с ИИ, к которым относятся:

- уполномоченные федеральных органов исполнительной власти (ФОИВ);
- органы управления программой (дирекция программы на базе головного разработчика/головного исполнителя образца ВВСТ);
- головной исполнитель (разработчик) образца ВВСТ в целом;
- головной изготовитель (если он не входит в состав головного исполнителя);
- исполнители (субподрядные организации, отвечающие за разработку алгоритмов ИИ);
- научно-исследовательские организации (НИО) государственных заказчиков и иные научные организации.

Наибольшее количество требований приходится на стадию эксплуатации, а также на стадии разработки и производства ВВСТ с ИИ. На начальных стадиях (формирование научно-технического задела и обоснование концепции ВВСТ с ИИ) основное внимание уделяется обоснованию ТТХ систем, на стадии утилизации — обеспечению конфиденциальности данных, накопленных за время функционирования системы с ИИ.

Основные виды возможных несоответствий различным группам требований, способы реагирования на них и ответственные субъекты управления ЖЦ ВВСТ с ИИ представлены в таблице 3.

Таблица 3

Особенности реагирования на выявленные несоответствия различным группам требований к ВВСТ с ИИ

№	Группа требований / Вид несоответствия	Возможные способы реагирования на несоответствие	Ответственный субъект управления ЖЦ
1	Состав и способы измерения характеристик ВВСТ с ИИ		
1.1	Некорректный состав учитываемых показателей качества алгоритмов ИИ (неполный, избыточные показатели)	Уточнение состава показателей качества алгоритмов ИИ	НИО государственных заказчиков
1.2	Некорректные веса частных показателей качества, используемые для определения интегрального показателя качества	Уточнение весов частных показателей качества, способов определения интегрального показателя качества	НИО государственных заказчиков
2	Формализация предусмотренных условий эксплуатации		
2.1	Некорректный состав существенных условий эксплуатации ВВСТ с ИИ (существенных факторов)	Уточнение состава существенных факторов	НИО государственных заказчиков
2.2	Неточная априорная оценка законов распределения существенных факторов в ходе эксплуатации ВВСТ с ИИ	Уточнение законов распределения	НИО государственных заказчиков
3	Унификация и обеспечение качества наборов данных		
3.1	Недостаточное качество (представительность) обучающих НД	Аугментация обучающих НД с учетом уточненных условий эксплуатации ВВСТ с ИИ	Исполнители НИОКР
3.2	Недостаточное качество (представительность) тестовых НД	Аугментация тестовых НД с учетом уточненных условий эксплуатации ВВСТ с ИИ	НИО государственных заказчиков

Продолжение таблицы 3

№	Группа требований / Вид несоответствия	Возможные способы реагирования на несоответствие	Ответственный субъект управления ЖЦ
4	Использование доверенных аппаратных средств		
4.1	Использование аппаратно-программных средств (АПС), не соответствующих требованиям в области информационной безопасности	Замена используемых АПС на доверенные отечественные, в случае невозможности — проведение сертификационных испытаний АПС в соответствии с установленным классом защищенности объекта автоматизации	Головной изготовитель ВВСТ с ИИ
5	Управление дообучением ВВСТ с ИИ на стадии эксплуатации		
5.1	Отсутствие возможности использования данных, формируемых в ходе эксплуатации, для дообучения ВВСТ с ИИ	Внесение изменений в систему технической эксплуатации ВВСТ с ИИ, предусматривающих возможность дообучения	Головной разработчик ВВСТ с ИИ
5.2	Неконтролируемая деградация качества ВВСТ с ИИ при дообучении на стадии эксплуатации	Доработка эксплуатационной документации, определяющей порядок подтверждения качества при дообучении ВВСТ с ИИ на стадии эксплуатации	Головной разработчик ВВСТ с ИИ
6	Обеспечение конфиденциальности данных		
6.1	Неконтролируемое повышение уровня конфиденциальности данных в процессе их обработки в ВВСТ с ИИ на стадии эксплуатации	Повышение класса защищенности объекта автоматизации (ВВСТ с ИИ) до необходимого	Уполномоченный ФОИВ
6.2	Нарушение конфиденциальности информации при утилизации ВВСТ с ИИ	Корректировка организационно-распорядительных документов, определяющих порядок утилизации образцов ВВСТ с ИИ	Уполномоченный ФОИВ
7	Масштабирование и тиражирование алгоритмов ИИ		
7.1	Недостаточная эффективность использования сформированных наборов и моделей данных на других прикладных задачах в сфере обороны и безопасности	Уточнение порядка формирования НД	НИО государственных заказчиков
8	Оценка функциональных возможностей квалифицированного человека-оператора		

Продолжение таблицы 3

№	Группа требований / Вид несоответствия	Возможные способы реагирования на несоответствие	Ответственный субъект управления ЖЦ
8.1	Отсутствие или некорректность оценок функциональных возможностей операторов, на автоматизацию деятельности которых направлено использование ИИ в ВВСТ	Проведение дополнительных исследований по оценке функциональных возможностей операторов при решении типовых прикладных задач	НИО государственных заказчиков
		Уточнение требований к ВВСТ с ИИ	Уполномоченный ФОИВ
9	Подготовка кадров		
9.1	Несоответствие квалификации эксплуатирующего персонала уровню сложности ВВСТ с ИИ	Корректировка профессиональных стандартов и образовательных программ в профильных учебных заведениях	Уполномоченный ФОИВ

Предложенная структура специфических требований в области ИИ позволяет ограничиться определением роли и места алгоритмов ИИ в комплексном объекте ВВСТ с распределением частных интеллектуальных задач по отдельным ФП, описанием связанной с этим специальной терминологии и формированием детальных требований к методам испытаний используемых в системе интеллектуальных алгоритмов. При этом вопросы комплексных испытаний не затрагиваются, что позволяет избежать дублирования требований в области механических и термических испытаний, электромагнитной совместимости, эргономики и других вопросов, относящихся к объекту автоматизации в целом.

Таким образом, в статье впервые с системных позиций были рассмотрены вопросы управления жизненным циклом образцов ВВСТ, использующих технологии искусственного интеллекта. На основе анализа процессов ЖЦ систем предложены принципы формирования и выявлены следующие основные группы требований к ВВСТ с ИИ:

- к составу и способам измерения существенных функциональных показателей и характеристик безопасности ВВСТ с ИИ;
- по формализации предусмотренных условий эксплуатации ВВСТ с ИИ;
- по унификации и обеспечению качества необходимых наборов данных;
- по использованию доверенных аппаратных средств;
- по управлению дообучением ВВСТ с ИИ на стадии эксплуатации;
- в области обеспечения конфиденциальности данных;
- по обеспечению возможности масштабирования и тиражирования алгоритмов ИИ на смежные прикладные интеллектуальные задачи в области обороны и безопасности;
- по оценке функциональных возможностей квалифицированных операторов, на автоматизацию деятельности которых направлено применение алгоритмов ИИ в ВВСТ;
- в области подготовки кадров.

Показано, что к наиболее представительным группам требований относятся характеристики и предусмотренные условия эксплуатации ВВСТ с ИИ. Унификация данных требований обеспечивается за счет использования классификатора интеллектуальных задач, основанного на аналогии ИИ и естественного интеллекта человека. Сформулированы особенности управления требованиями в зависимости от используемой модели жизненного цикла системы и в привязке к основным субъектам управления жизненным циклом ВВСТ.

ПРИМЕЧАНИЯ

[1] Указ Президента Российской Федерации от 7 мая 2012 г. № 603 «О реализации планов (программ) строительства и развития Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов и модернизации оборонно-промышленного комплекса».

[2] *Буренок В.М.* Проблемы создания системы управления полным жизненным циклом вооружения, военной и специальной техники // Вооружение и экономика. 2014. № 2 (27). С. 4—9.

[3] *Голубев С.С., Кукушкина Г.Р.* Проблемы развития системы управления полным жизненным циклом вооружения, военной и специальной техники. Экономика высокотехнологичных производств. Т. 1. 2020. № 4. Октябрь—декабрь. С. 183—196.

[4] *Звягин А.А.* На пороге перемен. Ч. 2. Элита развития. Преображение: монография. М.: ООО «Первое экономическое издательство», 2020. 292 с.

[5] Перспективная программа стандартизации в области приоритетного направления «Искусственный интеллект» на 2021—2024 годы. Утверждена 22 декабря 2020 г. URL: https://www.tc164.ru/Национальная-стандартизация (дата обращения: 10.09.2021).

[6] ГОСТ Р 56135-2014. Управление жизненным циклом продукции военного назначения. Общие положения.

[7] ГОСТ Р 57193-2016. Системная и программная инженерия. Процессы жизненного цикла систем (ISO/IEC/IEEE 15288:2015, NEQ).

[8] *Гарбук С.В.* Задачи нормативно-технического регулирования интеллектуальных систем информационной безопасности // Вопросы кибербезопасности. 2021. № 3 (43). С. 68—83.

[9] *Гарбук С.В., Бакеев Р.Н.* Конкурентная оценка качества технологий интеллектуальной обработки данных // Проблемы управления. 2017. № 6. С. 50—62.

[10] *Гарбук С.В.* Задачи нормативно-технического регулирования…

[11] ISO/IEC 24029-1-202X Information technology — Artificial Intelligence (AI) — Assessment of the robustness of neural networks. Part 1: Overview. ANSI. WD stage. 30 October 2019.

[12] ГОСТ Р ИСО/МЭК 19795-1-2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы. Ч. 1. Принципы и структура.

[13] *Гарбук С.В., Губинский А.М.* Искусственный интеллект в ведущих странах мира: стратегии развития и военное применение. М.: Знание, 2020, 590 с.

[14] ГОСТ Р ИСО/МЭК 19795-1-2007.

[15] *Гарбук С.В., Губинский А.М.* Искусственный интеллект…

[16] *Гарбук С.В.* Применение технологий искусственного интеллекта при разработке и эксплуатации ВВСТ // Сборник по итогам проведения научно-деловой программы Международного военно-технического форума «АРМИЯ-2018». 24—27 августа 2018 года.

[17] ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

[18] ГОСТ Р 56135-2014.

[19] Там же.

Высокоточные боеприпасы ствольной артиллерии, результаты полигонных испытаний, направления развития

Полковник А.Ю. БЕЖЕНЦЕВ,
кандидат технических наук

Майор А.Е. ПОЛЯКОВ

Подполковник в отставке В.М. ТУМАКОВ

АННОТАЦИЯ

Проведен анализ состояния отечественных высокоточных боеприпасов (ВТБ) для ствольной артиллерии с учетом результатов полигонных испытаний. Предложены пути их дальнейшего развития.

ABSTRACT

The paper analyzes the condition of domestic precision-guided ammunition (PGA) for barrel artillery, considering the results of field tests. It proposes ways of furthering PGA.

КЛЮЧЕВЫЕ СЛОВА

Высокоточные боеприпасы, ствольная артиллерия, артиллерийские комплексы, испытания, боевое применение.

KEYWORDS

Precision-guided ammunition, barrel artillery, artillery units, tests, combat employment.

ПРОИСХОДЯЩИЕ в настоящее время серьезные изменения в характере ведения боевых действий оказывают влияние на тенденции развития артиллерии. Самыми актуальными требованиями к артиллерии являются высокая точность, сочетающаяся с внезапностью и постоянной готовностью к открытию огня по обнаруженным целям. Наиболее полно данные требования выполняются при применении артиллерией высокоточных боеприпасов.

Разработка ВТБ для ствольной артиллерии в нашей стране и за рубежом началась в конце 60-х — начале 70-х годов XX столетия. На вооружение отечественной артиллерии приняты такие комплексы ВТБ как: «Смельчак», «Сантиметр», «Краснополь», «Китолов-2», «Китолов-2М», «Грань». Краткие характеристики перечисленных комплексов приведены в таблице.

Для комплексов «Смельчак» и «Сантиметр» в таблице указана вероятность попадания в круг с радиусами 6 м — «Смельчак» и 4,5 м — «Сантиметр», в центре которого находится цель. Данные комплексы, разработанные в московском Научно-исследовательском машиностроительном институте под руководством В.С. Вишневского, относятся к корректируемому управляемому артиллерийскому вооружению.

Наведение корректируемых ВТБ осуществляется на конечном участ-

Таблица

Характеристики артиллерийских комплексов ВТБ

Наименование комплекса	Индекс комплекса	Калибр, мм	Дальность стрельбы макс/мин, км	Масса снаряда, кг	Масса ВВ, кг	Вероятность попадания в цель
«Смельчак»	1К113	240	9,2/3,6	134,2	21,4	0,6
«Сантиметр»	2К24	152	12,0/0,5	49,5	8,5	0,8
«Краснополь»	2К25	152	20,0/3,0	50,8	6,6	0,8
«Китолов-2»	2К28	120	12,0/2,0	28,0	5,3	0,9
«Китолов -2М»	КМ3	122	12,2/2,0	28,3	5,3	0,8
«Грань»	КМ8	120	7,0/1,5	27,1	5,2	0,85

ке траектории, за 3—4 с до подлета снаряда (мины) к цели с помощью импульсных двигателей коррекции. Комплекс «Смельчак» прошел государственные испытания (ГИ) и принят на вооружение 31 декабря 1982 года.

В ходе боевых действий в Афганистане и проведения контртеррористической операции на Северном Кавказе «Смельчак» показал высокую эффективность. Так, в 2000 году для решения специальных задач сформировали отдельный дивизион, вооруженный самоходными минометами 2С4 «Тюльпан».

За три неполных месяца участия в боевых действиях дивизион выполнил более сотни огневых задач, уничтожив десятки особо прочных ДОТов, ДЗОТов, мостов, переправ и других важных целей. При выполнении огневых задач корректируемыми минами около 80 % объектов были разрушены полностью[1]. Корректируемая мина 3Ф5, входящая в комплекс, продолжительное время выпускалась серийно. В настоящее время она снята с производства, а сроки технической пригодности имеющихся запасов истекли.

Комплекс «Сантиметр» принят на вооружение в 1985 году. Корректируемый снаряд 3ОФ38, входящий в состав комплекса, выпущен в ограниченных объемах и практически не применялся, так как к этому времени уже проходил испытания управляемый комплекс «Краснополь». Снаряд 3ОФ38 так же, как и мина 3Ф5 промышленностью не выпускается, сроки технической пригодности запасов давно истекли.

Вместе с тем комплексы корректируемого вооружения обладают рядом преимуществ, к которым следует отнести:

- относительную дешевизну производства;
- простоту в эксплуатации и в использовании по назначению;
- короткое время подсвета цели;
- высокую эффективность боевой части (особенно мины 3Ф5). При разрыве мины в радиусе 15—20 метров от воронки обваливаются стенки траншей, а пыледымовое облако достигает в радиусе 100 м. Не случайно уцелевшие после огневого налета боевики могли вернуться в боеспособное состояние только через несколько часов, а иногда и недель[2].

Недостатками корректируемых комплексов являются:

- необходимость в пристрелке цели миной 3Ф5, приводящая к потере внезапности открытия огня;
- недостаточная дальность стрельбы.

В связи с этим комплексы корректируемого вооружения для ствольной артиллерии в Российской армии оказались невостребованными.

Одновременно с разработкой корректируемого вооружения в нашей стране создавались и управляемые артиллерийские комплексы. Основная особенность таких комплексов — непрерывное управление снарядом на конечном участке траектории с помощью аэродинамических рулей.

Все отечественное управляемое артиллерийское вооружение создавалось в Конструкторском бюро приборостроения (г. Тула), под руководством А.Г. Шипунова — руководителя и главного конструктора предприятия. Особое место в ряду управляемых ВТБ отечественной ствольной артиллерии заслуженно занимает комплекс «Краснополь», принятый на вооружение в 1986 году.

Управляемый артиллерийский снаряд (УАС) 3ОФ39, входящий в комплекс «Краснополь», выпускался серийно с момента принятия на вооружение и до 2000 года. Комплекс в большом количестве поставлялся в ряд зарубежных стран: Китай, Индию, Венесуэлу. Неоднократно он успешно применялся в демонстрационных стрельбах, проводимых как в России, так и за рубежом.

Вместе с тем следует отметить, что комплекс в целом оказался сложным для освоения войсковыми расчетами. Для его успешного применения необходимо:

• соблюдение особенностей подготовки данных для стрельбы;

• установление соответствующих режимов частот на лазерном целеуказателе-дальномере (ЛЦД) и УАС;

• наличие у операторов практических навыков в работе с ЛЦД при стрельбе УАС;

• наличие исправной и соответствующей требованиям технических условий наземной аппаратуры комплекса: средств синхронизации выстрела (ССВ) и ЛЦД.

С учетом данных обстоятельств и в связи с тем, что у выпущенных ранее и находящихся на хранении боеприпасов истекал срок гарантийного хранения, данный комплекс стал применяться ограниченно, в основном на испытательных полигонах в исследовательских целях.

Так, в июле 2016 года в целях оценки основных тактико-технических характеристик УАС 3ОФ39 «Краснополь» провели экспериментальные стрельбы, используя для подсвета целей беспилотные летательные аппараты (БПЛА).

В ходе проведенных испытаний проверялись:

• возможности применения БПЛА для поиска, обнаружения и определения координат целей и обеспечения их подсвета с необходимой точностью в течение заданного времени;

• характеристики точности наведения УАС 3ОФ39 на цели (щит размером 3×3 м и танк) при облучении их подсветчиком, установленным на гиростабилизированной платформе БПЛА.

Кроме этого, оценивалась стабильность удержания пятна подсвета на цели во время пролета БПЛА в районе цели.

При проведении испытаний получены прямые попадания в цель, а также в круг с радиусом, не превышающим размер зоны гарантированного поражения не укрытой живой силы (~ в 45 % случаев), что подтвердило возможность использования БПЛА для обнаружения, определения координат целей с необходимой точностью и обеспечения их подсвета.

В ноябре-декабре 2016 года под руководством ГРАУ Министерства обороны проводились испытания (контрольный отстрел) боеприпасов «Краснополь» разных партий с истекшими сроками технической пригодности. Стрельба преимущественно велась на максимальную дальность по цели типа «танк» и по щитам раз-

Все отечественное управляемое артиллерийское вооружение создавалось в Конструкторском бюро приборостроения (г. Тула), под руководством А.Г. Шипунова — руководителя и главного конструктора предприятия. Особое место в ряду управляемых ВТБ отечественной ствольной артиллерии заслуженно занимает комплекс «Краснополь», принятый на вооружение в 1986 году.

мерами 1,5×1,5 м, находящимся на удалении 2—4 км от ЛЦД.

В результате стрельб получено значение вероятности прямого попадания в цель с первого выстрела не менее 0,7 при установленной опытной вероятности безотказной работы — 0,67.

Необходимо отметить, что иногда стрельба проводилась в сложных метеорологических условиях, характеризующихся низкой облачностью, атмосферными осадками (дождь, снег), недостаточной видимостью цели (туман, дымка, сумерки). Полученные положительные результаты испытаний свидетельствуют о том, что установленные регламентирующими документами ограничения на применение УАС «Краснополь» по метеорологическим условиям стрельбы могут быть пересмотрены.

В боевых условиях комплекс «Краснополь» применялся ограниченно. Известно, что в 1990-х годах во время вооруженного конфликта между Эфиопией и Эритреей двумя УАС 3ОФ39 прямыми попаданиями с первого выстрела уничтожено два танка[3].

Теперь комплекс «Краснополь» успешно применяется в Сирии. Так, в 2018 году при проведении операции по ликвидации бандформирований, напавших на авиабазу Хмеймим, ударом одного такого снаряда уничтожен неприятельский склад беспилотников.

В своем выступлении на расширенном заседании Комитета Госдумы по обороне Министр обороны генерал армии С.К. Шойгу отметил: «…В современных условиях все большее развитие приобретают беспилотные летательные аппараты. Стремительное развитие данные системы получают в военной области. Качественный рывок в развитии беспилотной авиации создал новые возможности разведки и поражения объектов противника. Так, благодаря лазерной подсветке с беспилотников удалось дать вторую жизнь ранее не востребованным высокоточным артиллерийским снарядам «Краснополь»…»[4].

Как показывает практический опыт применения комплекса «Краснополь», боевые и технические возможности комплекса далеко не исчерпаны и в настоящее время востребованность в нем растет.

Преимущества комплекса «Краснополь»:

- стрельба на поражение цели без пристрелки при подготовке данных на основе полной или сокращенной подготовки;
- высокая вероятность попадания в цель с первого выстрела;
- мощное действие боевой части;
- большая зона выбираемых ошибок подготовки данных для стрельбы;
- возможность применения БПЛА для подсвета цели;
- высокая надежность выстрела.

Существенными недостатками комплекса являются:

- необходимость длительной подсветки цели лазерным целеуказателем-дальномером (около 15 с);

• опасность поражения своих войск при стрельбе через их позиции.

Управляемые комплексы «Китолов-2», «Китолов-2М» и «Грань» разработаны в начале 2000-х годов с использованием базы своего предшественника УАС «Краснополь».

Комплекс 2К28-«Китолов-2» разработан для 120-мм орудий 2С9, 2С9-1, 2С23. Принят на вооружение в 2002 году, выпущен серийно, но в незначительных объемах.

Комплекс управляемого вооружения КМ-3, «Китолов-2М» создан для 122-мм орудий Д-30, а комплекс КМ-8 «Грань» — для 120-мм минометов. Данные системы разрабатывались в целях поставок за рубеж и на вооружение Российской армии не принимались.

Все отечественные ВТБ ствольной артиллерии оснащены полуактивной лазерной системой наведения (ПЛГСН), что является их главным недостатком. Стрельбу ими можно вести только по наблюдаемым целям при отсутствии в створе лазерного излучения экранирующих предметов. Продолжительная работа ЛЦД на наблюдательном пункте в режиме подсвета цели обусловливает высокий риск его обнаружения противником.

Вместе с тем у данных боеприпасов есть неоспоримое преимущество над боеприпасами с системой наведения по сигналам от спутниковых навигационных систем. Стрельба снарядами с ПЛГСН может производиться по целям, разведанным с большой ошибкой в определении координат (до сотен метров), а также по отдельным целям, входящим в состав групповой, без смены установок для стрельбы.

В целях дальнейшего развития ВТБ с ПЛГСН было бы целесообразно:

• включить в инструкцию по боевой работе возможность выбора способа синхронизации начала работы ЛЦД с моментом выстрела. В настоящее время команда на включение ЛЦД подается с огневой позиции в момент выстрела. В случае, когда команда на включение ЛЦД не поступает, например, из-за помех в радиосвязи, цель при подлете к ней УАС не подсвечивается, происходит промах. Такие события в ходе испытаний наблюдались неоднократно;

• разработать малогабаритный (не более 1,5—2 кг) лазерный целеуказатель-дальномер для тактических групп, действующих в непосредственном соприкосновении с противником;

• включить (придать) в артиллерийские подразделения расчеты БПЛА, осуществляющие разведку местности, корректирующие стрельбу и подсвечивающие цели при применении управляемых снарядов;

• разработать относительно недорогую корректируемую (управляемую) мину 120-мм и 82-мм калибра, что позволит более широко применять высокоточные боеприпасы при ведении боевых действий в населенных пунктах;

• поставить в войска специальные тренажеры, моделирующие боевую работу артиллерийских расчетов при применении ВТБ.

Разработка и производство ВТБ — это наукоемкие, дорогостоящие и технологически сложные работы, ведущиеся в настоящее время во всех развитых государствах, в том числе и в России.

В нашей стране успешно проходит испытания УАС «Краснополь-М2», представляющий собой глубокую модернизацию комплекса «Краснополь». Тактико-технические характеристики нового образца значительно превосходят показатели своего предшественника, и есть уверенность в том, что он будет принят на вооружение Российской Армии.

На рисунках 1, 2, 3 представлены фрагменты видеосъемки испыта-

ний комплекса «Краснополь-М2». Стрельба велась одновременно по двум целям залпом из двух орудий. Подсвет мишеней осуществлялся с наземного пункта двумя ЛЦД, работающими на разных режимах излучения. На рисунке 1 представлена мишенная обстановка до открытия огня. На рисунке 2 зафиксирован момент попадания первого снаряда в мишень и момент подхода второго снаряда (красная полоса — след от работы газогенератора) к танку. На рисунке 3 зафиксировано прямое попадание второго снаряда в цель.

Рис. 1. Вид мишенной обстановки

Рис. 2. Момент поражения мишени

Рис. 3. Результат стрельбы УАС «Краснополь-М2» залпом из двух орудий

Вместе с тем необходимо отметить, что все рассмотренные комплексы относятся к ВТБ первого поколения. За рубежом ведутся работы по созданию высокоточных боеприпасов третьего поколения, характеризующихся принципом «выстрелил—забыл». Наведение таких боеприпасов осуществляется: на траектории — по спутниковым навигационным полям, а при подлете к цели — активной (пассивной) головкой самонаведения. Особое внимание уделяется разработке управляемых дальнобойных снарядов.

Так, армия США в рамках программы создания перспективного артиллерийского комплекса с повышенной дальностью стрельбы подписала контракт на разработку и производство снаряда XM1155 «Эскалибур». Активно-реактивный 155-мм снаряд с аэродинамическими рулями управляется системой инерциальной и спутниковой навигации. Планируется, что им можно будет поражать как неподвижные, так и подвижные цели, находящиеся на суше и на море на дальностях свыше 100 км[5].

Говоря об условиях проведения полигонных испытаний ВТБ в настоящее время, приходится констатировать, что при создании первых отечественных управляемых снарядов материально-техническое обеспечение этого процесса было полнее. Сегодня обеспечение испытаний в основном осуществляется на договорной основе и в минимально допустимых объемах. Не хватает опытных специалистов из числа гражданского персонала. Все это сказывается на качестве проводимых испытаний.

Разработка и производство ВТБ — это наукоемкие, дорогостоящие и технологически сложные работы, ведущиеся в настоящее время во всех развитых государствах, в том числе и в России. В нашей стране успешно проходит испытания УАС «Краснополь-М2», представляющий собой глубокую модернизацию комплекса «Краснополь». Тактико-технические характеристики нового образца значительно превосходят показатели своего предшественника, и есть уверенность в том, что он будет принят на вооружение Российской Армии.

Высокоточное оружие, в том числе и ВТБ ствольной артиллерии, характеризуют мощь и уровень научно-технического потенциала государства и его Вооруженных Сил. Учитывая мировые тенденции развития средств вооруженной борьбы, изменения характера боевых действий, необходимо активизировать работы по созданию перспективных и модернизации ранее созданных образцов управляемых боеприпасов для Вооруженных Сил России.

ПРИМЕЧАНИЯ

[1] Ломаченко С.В., Булатов О.Г., Гаврилович С.Л. Артиллерия большой мощности: история и перспективы развития // Военная Мысль. 2001. № 2. С. 5, 7.

[2] Там же.

[3] Коровин В.Н. Аркадий Шипунов. Тула: Дизайн-Коллегия, 2008. С. 474.

[4] Курс — лучшая армия мира // Национальная оборона. 2019. № 3. С. 28.

[5] Зарубежное военное обозрение. 2020. № 7. С. 95.

Беспарашютное десантирование как элемент трансформации подготовки войск и командных кадров

Полковник запаса А.В. ЗЕЛЕНОВ,
кандидат военных наук

Полковник запаса А.В. ВДОВИН,
кандидат военных наук

АННОТАЦИЯ

Рассмотрена взаимообусловленность способов десантно-штурмовых действий с обучением войск и командных кадров — курсантов РГВВДКУ, а также специалистов воздушно-десантной подготовки беспарашютному десантированию. Показан подход к созданию и функционированию специализированной учебно-материальной базы.

ABSTRACT

The paper examines mutually conditioned methods of landing and assault activity and troop and commander training of cadets at Ryazan Higher Airborne Command School of the Guards, and also of specialists in airborne training and parachuteless landing.

КЛЮЧЕВЫЕ СЛОВА

Беспарашютное десантирование, десантно-штурмовые формирования, воздушно-десантная подготовка подразделений ВДВ и курсантов-десантников (специалистов), воздушно-десантный (штурмовой) комплекс.

KEYWORDS

Parachute-free landing, airborne assault formations, airborne training of airborne units and paratrooper cadets (experts), airborne (assault) complex.

А.В. ЗЕЛЕНОВ, А.В. ВДОВИН

АНАЛИЗ характера вооруженной борьбы на современном этапе между- и внутригосударственных отношений дает основание полагать, что одной из основных тенденций ее развития выступает повышение мобильности войск и прежде всего аэромобильности, способствующей переносу и сосредоточению усилий на различных направлениях в короткие сроки. Создание десантно-штурмовых формирований «нового типа» подтвердило правильность проведенных исследований в контексте востребованности указанного компонента войск в составе группировки войск (сил) быстрого реагирования. В свою очередь, десантно-штурмовые действия как форма боевого применения десантно-штурмовых подразделений и частей предопределили потребность выработки новых тактических приемов действий десанта во взаимодействии с вертолетами, наибольшие изменения в которых относятся к периоду его высадки.

Типовые способы десантно-штурмовых действий предусматривают нанесение противнику поражения ударами беспилотной и армейской авиации при поддержке самолетами оперативно-тактической авиации с последующим проведением главными силами десантно(воздушно)-штурмовой атаки в разных (или с нескольких направлений) по захвату и уничтожению назначенных объектов противника с одновременным выделением части сил на прикрытие (для демонстрационных действий) и нанесением ударов армейской авиации по подходящим резервам противника или проведение десантно(воздушно)-штурмовой атаки в одном направлении для захвата и уничтожения назначенных объектов противника с одновременной высадкой части сил для захвата и удержания назначенного района. Одним из направлений их совершенствования является высадка десанта с вертолетов в сложных метеоусловиях на различные типы местности, в том числе ограниченные участки и сооружения в любое время суток, а также в режиме пролета, т. е. с ходу.

Сущность десантно-штурмовой атаки при этом заключается в нанесении по противнику внезапных и стремительных ударов с разных направлений подразделениями десанта в звене «рота—взвод», высаженными с вертолетов, в сочетании с одновременными ударами большей части боевых и транспортно-боевых вертолетов, а также в осуществлении при необходимости широкого маневра силами и средствами десанта по воздуху.

В основе произошедших при этом изменений содержится способность беспарашютного десантирования личного состава в места выполнения учебно-боевых, боевых и специальных задач без посадки вертолетов на грунт (площадки приземления), а также его эвакуации из труднодоступных районов местности, в том числе и с водной поверхности. По своей сущности «беспарашютное десантирование» — это высадка военнослужащего (спуск груза) с определенной высоты из неподвижного, относительно земли (воды), вертолета без использования парашютных систем. В отличие от классического парашютного десантирования указанный способ выполняется с помощью спусковых устройств (шнуров) и специальных канатов (штурмо-

вой — 6 м и десантно-эвакуационные — 18 и 25 м, на фото 1 и 2), как правило, в труднодоступной сильнопересеченной местности, не обеспечивающей посадку вертолетов на грунт[1].

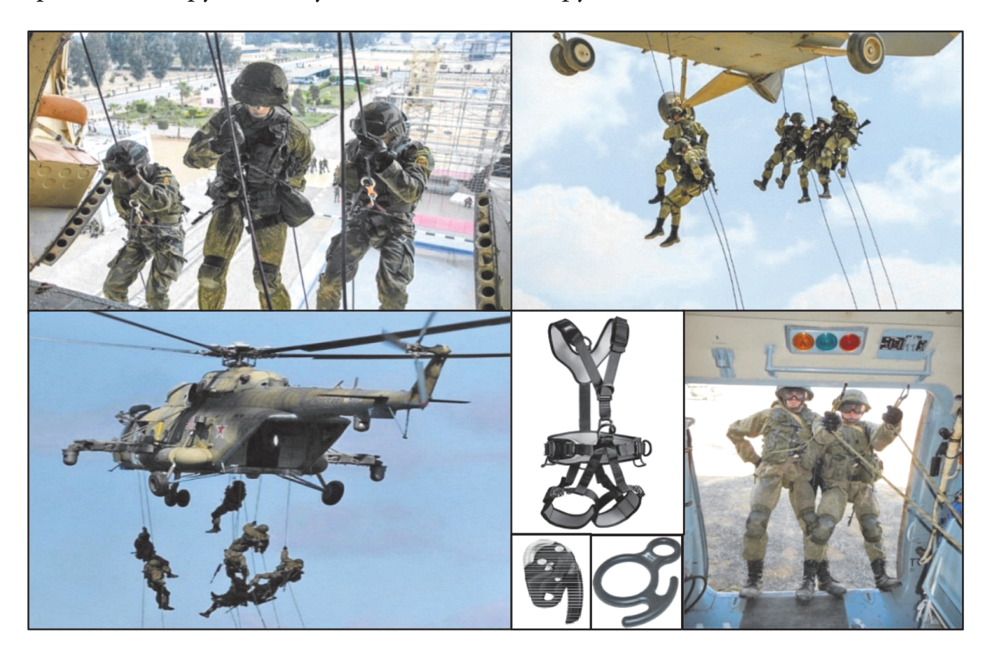


Фото 1. Высадка с помощью спусковых устройств

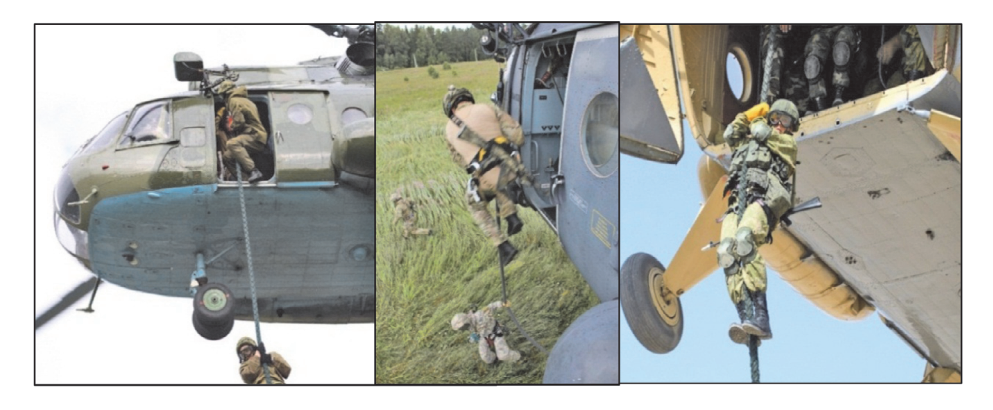


Фото 2. Десантирование с помощью канатов

При этом возможность предшествующего беспарашютному десантированию личного состава спуска грузов способствует доставке десанта в район выполнения задачи с запасами материальных средств (дополнительным оружием, боеприпасами и снаряжением), упакованными в малогабаритную тару, а также их дополнительную подачу в ходе боя.

Кроме того, поступающее на снабжение оборудование транспортно-боевых вертолетов допускает эвакуацию личного состава в режиме висения вертолета без его посадки, а также экстренную эвакуацию пострадавших и раненых на канате и спасательных платформах, размещаемых на внешней подвеске вертолетов, с использованием электролебедок (фото 3).

Фото 3. Эвакуация с использованием каната и подвесной спасательной платформы

В свою очередь, внедрение в практику подготовки войск новых средств десантирования непосредственно влияет на подготовку кадров, основными направлениями которой выступает подготовка инструкторов беспарашютного десантирования, выпускающих, а также начальная подготовка личного состава и ее совершенствование.

Происходящие изменения предопределили потребность внесения соответствующих изменений и корректировок в существующие системы боевой подготовки войск и подготовки командных кадров для ВДВ в военных вузах. Вследствие этого в ВДВ разработана программа подготовки личного состава к беспарашютному десантированию и внесены соответствующие изменения в программы боевой подготовки десантно-штурмовых подразделений, а группой военного образования — в программы обучения курсантов.

Соответствующая подготовка инструкторов беспарашютного десантирования организована на базе Рязанского гвардейского высшего воздушно-десантного командного училища имени генерала армии В.Ф. Маргелова.

Для обучения по разработанной программе в рамках дополнительного профессионального образования назначены штатные инструкторы беспарашютного десантирования, заместители командиров десантно-штурмовых, разведывательных рот и рот специального назначения, заместители командиров десантно-штурмовых и разведывательных батальонов соединений и воинских частей ВДВ.

Подготовка выпускающих и начальная подготовка личного состава воинских частей по беспарашютному десантированию организована подготовленными инструкторами в ходе учебных сборов в воинских частях, а курсантов высшего профессионального образования РГВВДКУ — на учебных занятиях в училище. При этом в течение учебного года спланированы занятия по выполнению не менее 20 практических спусков с использованием тренажеров и не менее четырех спусков из вертолета Ми-8 с высот от 25 до 40 м.

Дополнительно появившиеся задачи воздушно-десантной подготовки специалистов, личного состава подразделений и курсантов образовательных организаций по

выполнению беспарашютного десантирования предопределили соответствующую направленность их подготовки, в частности[2]:

• выработку единой методики организации и проведения теоретических и практических занятий по выполнению спусков (подъемов);

• формирование практических навыков выполнения спусков из вертолета с использованием спусковых устройств и канатов в рамках выполнения учебно-боевых и боевых (специальных) задач;

• формирование практических навыков выполнения спусков (подъемов) людей (грузов) с применением бортовых грузовых электролебедок.

Собственно же подготовка специалистов воздушно-десантной службы (подготовки), личного состава образовательных организаций и подразделений, в том числе авиационных, к выполнению беспарашютного десантирования, включающая традиционные теоретическую и наземную подготовки, а также практическое выполнение спусков, разработана и проводится, как правило, в восемь этапов[3].

Первый — теоретическая и наземная подготовка к выполнению спусков.

Теоретическая подготовка проводится в специализированных классах в целях получения военнослужащими знаний в области беспарашютного десантирования и эвакуации с помощью спусковых устройств и канатов. При этом изучаются виды используемого снаряжения, его технико-эксплуатационные характеристики, комплектность, основные критерии хранения, эксплуатации и отбраковки спусковых устройств (канатов), необходимая экипировка и требования безопасности при выполнении спусков.

В свою очередь, наземная подготовка личного состава проводится на специальных воздушно-десантных комплексах (парашютных городках, макетах вертолетов) для совершенствования умений и навыков, необходимых для выполнения спусков. При ее проведении изучаются правила безопасной эксплуатации используемого снаряжения, подгонка экипировки, основные используемые узлы, порядок укладки шнуров (канатов), а также отрабатываются элементы спусков и действия в особых случаях.

Второй — постановка командиром десантно-штурмового формирования задач участникам мероприятия на подготовку личного состава, вертолетов, необходимого имущества, снаряжения и средств обеспечения спусков.

Третий — предварительная подготовка к выполнению спусков, проводимая начальником ВДС (ВДП) или назначенным им руководителем спусков. Реализуемый при этом комплекс мероприятий и действий войск предусматривает разработку документации и постановку задачи личному составу, проведение занятия по изучению техники выполнения спусков и действий в особых случаях, соответствующие тренажи на специальных воздушно-десантных комплексах, а также подготовку имущества, снаряжения и обмундирования.

Четвертый — контроль готовности (знаний) каждого спускающегося, в том числе лиц из числа выпускающих и наряда по руководству и обеспечению спусков.

Пятый — предспусковая подготовка к выполнению спусков в день (ночь) выполнения спусков, основным содержанием которой выступает подготовка своего снаряжения к выполнению спусков и наземная отработка элементов спусков (подъемов) на вертолете совместно с экипажем.

Шестой — проведение полетов с выполнением спусков.

Седьмой — разбор организации и проведения спусков.

Восьмой — оформление документации по итогам выполненных полетов и спусков.

Сформированные при этом умения и навыки (способности) являются важным компонентом боевой подготовки войск и образовательной деятельности обучающихся в контексте их профессиональной деятельности.

Полученный при этом опыт способствует совершенствованию и развитию организационной структуры десантно-штурмовых формирований, разработке и реализации сбалансированной программы подготовки личного состава к десантированию, формированию эффективных тактических приемов совместных (коллективных) действий десантников с и на вертолетах с использованием средств беспарашютного десантирования.

Соответствующие изменения программ боевой подготовки и образовательного процесса военных вузов предопределили потребность создания соответствующей учебно-материальной базы. Так, для подготовки личного состава подразделений к беспарашютному десантированию в воинских частях создается комплекс беспарашютного десантирования с включением в него тренажера-вышки, высотных тренажеров «Вертолет Ми-8» и тренажеров «Вертолета Ми-8» на (фото 4)[4].

Фото 4. Тренажерный комплекс беспарашютного десантирования с вертолетов

В свою очередь, для повышения эффективности проведения учебных мероприятий, увеличения количества и качества тренировок разработан комплекс отработки беспосадочного способа доставки с применением альпинистского снаряжения и канатов для скоростного спуска, а также эвакуации, в том числе раненых и пострадавших, на основе вертолета Ми-8, имитирующий движение и зависание вертолета, внедрение которого способствует экономии ресурса служебной авиатехники и, соответственно, значительной экономии затрат на подготовку личного состава.

Указанный тренажер (фото 5), управляемый одним сотрудником без навыков пилотирования, обеспечивает не только обучение выпускающего стандартным способам беспарашютного десантирования, но и моделирование всевозможных неш-

Фото 5. Динамический тренажер для беспарашютного десантирования

татных ситуаций без потерь личного состава и авиатехники.

Усложненные спуски (подъемы), в частности, ночью, на воду, лед (мерзлый грунт), лес, площадки приземления ограниченных размеров (крышу здания, палубу судна и т. п.) или имеющие препятствия (неровности поверхности) высотой более 0,5 м, движущиеся объекты, при скорости ветра у земли 10 м/с и более, с высоты 30 м и более, с вооружением (кроме пистолета) и (или) рейдовым рюкзаком (грузовым контейнером) из вертолета, двигающегося с поступательной скоростью до 10 км/ч, а также с выполнением обязанностей выпускающего предопределяют потребность комплексирования создаваемой учебно-материальной базы в рамках штурмового комплекса, вариант которого, разработанный в преддверии совместных египетско-российских антитеррористических учений «Защитники дружбы-2018», представлен на фото 6.

Для повышения эффективности проведения учебных мероприятий, увеличения количества и качества тренировок разработан комплекс отработки беспосадочного способа доставки с применением альпинистского снаряжения и канатов для скоростного спуска, а также эвакуации, в том числе раненых и пострадавших, на основе вертолета Ми-8, имитирующий движение и зависание вертолета, внедрение которого способствует экономии ресурса служебной авиатехники и, соответственно, значительной экономии затрат на подготовку личного состава.

После обучения действиям при проведении беспарашютного десантирования на снарядах воздушно-десантного комплекса проводятся тренировки практических спусков с 10-метровых вышек скалодрома сначала в медленном темпе в одиночных спусках, затем — тренировки в составе группы со скоростью не более 3 м/с (фото 7).

Фото 6. Устройство штурмового комплекса в Арабской Республике Египет: 1 — тренажер для беспарашютного десантирования, 2 — лесной массив для спусков, 3 — здание для спусков на крышу, 4 — площадка для спусков на твердую поверхность, 5 — бассейн для спусков на воду, 6 — макет корабля для спусков на судно, 7 — горно-штурмовой комплекс

Фото 7. Тренировка в спуске личного состава и груза на 10-метровой вышке скалодрома

Таким образом, разрабатываемый типовой десантно-штурмовой комплекс для отработки беспарашютного способа высадки личного состава с применением спусковых устройств и специальных десантных канатов призван обеспечивать подготовку десантников как при одиночном спуске, так и при спусках в составе группы от момента отделения от летательного аппарата до приземления в заданную точку при различных типовых усло-

виях, включая действия в нештатных ситуациях.

В свою очередь, опробованная в ходе учений способность, наряду с традиционным десантированием личного состава, ВВСТ и запасов материальных средств десанта внутри грузовой кабины вертолетов, доставки их в тыл противника на внешней подвеске (фото 8), предопределила трансформацию содержания подготовки войск и соответствующих командных кадров и по другим учебным дисциплинам, в первую очередь таким, как тактическая, огневая и техническая в контексте реализуемых способов выполнения десантом боевой задачи.

Фото 8. Переброска техники и грузов на внешней подвеске вертолетов

Таким образом, необходимо отметить, что задача профессиональной подготовки командных кадров становится одной из приоритетных и главных, что, в свою очередь, предусматривает непрерывное развитие и совершенствование соответствующих программ обучения (подготовки), методик организации и проведения учебных занятий и тренировок, имитационных технических средств обучения, а также разработки новых и модернизации существующих тренировочных средств. Компетентность соответствующих специалистов выступает основой эффективной реализации ими способов боевого применения десантно-штурмовых формирований.

ПРИМЕЧАНИЯ

[1] Руководство по беспарашютному десантированию (РБПД-2020). М.: Командование ВДВ, 2020.

[2] Инструкция по беспарашютному десантированию с помощью спусковых устройств и специальных канатов из вертолетов армейской авиации для военнослужащих ВДВ и подразделений специального назначения. М.: Командование ВДВ, 2020.

[3] Инструкция по подготовке и выполнению учебно-тренировочных и боевых спусков на спусковых устройствах для военнослужащих воздушно-десантных войск и подразделений специального назначения. М.: Командование ВДВ, 2019.

[4] Тактико-технические требования, предъявляемые к тренажерам для беспарашютного десантирования. М.: Командование ВДВ, 2020.

Организация подготовки подразделений и органов управления с использованием комплексных тактических тренажеров

Полковник в отставке Н.Н. ЛЕВЕНТОВ,
кандидат военных наук

Полковник в отставке Н.Д. АЛЁШЕЧКИН,
кандидат технических наук

Полковник в отставке А.В. АНАСТАСИН,
кандидат военных наук

АННОТАЦИЯ

Обосновывается необходимость и целесообразность создания и внедрения в процесс боевой учебы Сухопутных войск комплексных тактических тренажеров в интересах повышения качества подготовки батальонных тактических групп к выполнению задач по предназначению. Особое внимание уделено рассмотрению условий, обеспечивающих их встраиваемость в существующую систему боевой подготовки (в части ее организации).

ABSTRACT

The paper substantiates the need and expediency of creating integrated tactical simulators to be introduced in the process of combat training of the Ground Forces in the interests of improving the standards of battalion tactical groups' readiness for accomplishing missions as intended. Particular attention is given to conditions that ensure their integration in the existing system of combat training (as regards its organization).

КЛЮЧЕВЫЕ СЛОВА

Комплексный тактический тренажер, программа боевой подготовки, единая комплексная тактическая задача, комплексный подход, модульная организация боевой подготовки.

KEYWORDS

Integrated tactical simulator, combat training program, uniform integrated tactical task, integrated approach, modular organization of combat training.

СПЕЦИАЛЬНАЯ военная операция на территории Украины в полной мере высветила важность подготовки батальонных тактических групп (БТГр) Сухопутных войск (СВ), которым принадлежит ведущая роль в достижении поставленных целей, а их командиры несут особую ответственность за успешное решение боевых задач при заданных условиях сохранения жизней мирных граждан.

Трудности в подготовке БТГр были известны и ранее, поэтому вопросы поиска путей решения назревших проблем прежде неоднократно поднимались авторами настоящей статьи. Но непосредственным поводом вновь уделить внимание данной теме послужил ряд мероприятий, на которых

в том или ином контексте рассматривались новые подходы к решению проблемных вопросов боевой подготовки войск и корректировалось содержание уже решаемых задач.

Так, в ходе прошедшего в марте 2022 года выездного заседания Совета главных конструкторов по техническим средствам обучения (ТСО) системы вооружения сухопутной составляющей сил общего назначения на его секции № 2 «Обучающие тренажерные средства ВВСТ» обсуждались вопросы совершенствования подготовки БТГр с использованием ***комплексных тактических тренажеров*** (КТТ). Мероприятие, проводившееся на территории тульского предприятия АО «Тулаточмаш», стало, по сути, развернутым продолжением обсуждения вопросов, ранее затронутых в ходе конференций, состоявшихся в рамках Международного военно-технического форума «Армия-2021». Оно позволило участникам всесторонне обсудить подходы к созданию КТТ на основе современных технологий, оценить реалистичность основных идей и принять ряд важных решений, направленных на их реализацию.

Батальонная тактическая группа в текущий момент и на обозримую перспективу является основным тактическим формированием в СВ. От качества их полевой выучки непосредственно зависит боевая способность данного вида Вооруженных Сил РФ в целом. Поэтому на приоритетной подготовке БТГр необходимо сосредоточить главные усилия в деятельности командующих и командиров всех уровней.

Известно, что высшей формой подготовки войск считаются тактические учения (ТУ), а органов управления — командно-штабные учения (КШУ) с привлечением войск. При их проведении в максимально возможной в мирное время степени воссоздаются условия реального боя. Однако главная условность любого учения, связанная с отсутствием реального противодействия противника, сохраняется. К тому же данные мероприятия боевой подготовки требуют серьезных финансовых и материальных затрат.

В связи с этим на экспертном уровне признано, **что создание и внедрение КТТ — наиболее перспективное направление повышения качества подготовки БТГр для выполнения задач по предназначению**. При такой постановке вопроса КТТ рассматривается как совокупность тренажерных и программно-технических средств, объединенных в единое информационное пространство и предназначенных для слаживания подразделений и органов управления тактического звена. На наш взгляд, занятия и учения с использованием КТТ позволят развивать у командиров подразделений способность предвидеть ход и исход общевойскового боя как при его подготовке, так и в динамике, а также умение оценивать еще до боевого столкновения с противником, насколько эффективным окажется тот или иной тактический прием или способ выполнения боевой задачи.

По существующей классификации учебной материальной базы (УМБ) боевой подготовки КТТ относится к ее классному сегменту, который позволяет обучать подразделения, офицеров и органы управления с наименьшими финансовыми организационными, временными, транспортными и другими затратами. Вместе с тем в ходе обсуждения и оценки реального состояния классных тренажеров специалисты приходят к заключению, что на перспективу предпочтительнее создавать элементы КТТ в контейнерном исполнении. Данный вариант построения КТТ имеет целый ряд преимуществ перед классным (стационарным). В частности,

он обладает транспортабельностью, и, следовательно, его легко переместить с одного операционного направления на другое в соответствии с текущей потребностью, а также способностью к гибкому конфигурированию состава и структуры, т. е. из отдельных модулей-контейнеров можно создавать тренажеры необходимого масштаба — от отделения и взвода до бригадного уровня.

У разработчиков КТТ имеется ясное понимание, что данное средство обучения является наиболее сложным и дорогостоящим компонентом в системе ТСО СВ, поэтому цена возможных ошибок при его проектировании может оказаться высокой. **Лидирующее положение КТТ среди других тренажеров предопределено его ролью как связующего звена между традиционными и новыми формами подготовки войск, основанными на применении современных технологий, включая искусственный интеллект (ИИ).**

Однако даже новейшие учебно-тренировочные средства (УТС) — это всего лишь инструменты, позволяющие обучаемым быстрее овладевать необходимыми умениями и навыками для успешного выполнения задач по предназначению. Требования к организации боевой подготовки и ее содержанию изложены в программах боевой подготовки, которые регламентируют построение процесса обучения военнослужащих и слаживания подразделений. Тем не менее сами по себе они не дают исчерпывающих отправных положений для организации подготовки подразделений. Их содержание уточняется, дополняется и расширяется другими руководящими документами: приказами, организационно-методическими указаниями, директивами и др. В полку и бригаде документом, суммирующим все требования данных документов, является ***Единая комплексная тактическая задача*** (ЕКТЗ).

В Наставлении по боевой подготовке в Вооруженных Силах РФ обращается внимание, что при практической отработке ЕКТЗ необходимо «последовательное наращивание обстановки от одного занятия к другому по единому тактическому замыслу применительно к боевым задачам»[1]. Командир полка или бригады, обучая БТГр, обязан исходить из того, что «любое последующее мероприятие, проводимое в рамках ЕКТЗ, должно быть логическим продолжением предыдущего»[2].

При этом ЕКТЗ — не только «совокупность требований к содержанию, объему и срокам выполнения мероприятий, предназначенных для отработки в полном объеме программ боевой подготовки»[3], но и документ, содержательно определяющий порядок подготовки соединения (воинской части) к главному мероприятию в учебном году — тактическому учению. По сути, ЕКТЗ — инструмент, позволяющий добиться объединения усилий по трем основным направлениям боевой учебы: подготовке органов управления (штабов), офицеров и подразделений в целях обеспечения готовности воинской части, соединения к выполнению боевых задач по предназначению или внезапно возникших боевых (специальных) задач в ограниченные сроки.

Полагаем, что **для реализации требований к подготовке подразделений, офицеров и органов управления, отраженных в ЕКТЗ, необходим комплексный подход**. Его сущность заключается в последовательном согласовании (синхронизации) по тематике и времени проведения ТУ, КШУ, групповых упражнений, тактических летучек, штабных тренировок, что позволяет в полном объеме раскрыть содержание и достичь цели отработки каждого модуля — учебно-боевой задачи.

При этом решение командира и другие планирующие документы,

разрабатываемые штабом воинской части (соединения), становятся основой для отработки документов и подготовки нижестоящих органов управления (штабов), офицеров, подразделений. Все занятия в рамках комплексного подхода проводятся в единой тактической обстановке. Командиры низших уровней (батальона, роты, взвода, отделения) не создают исходную обстановку самостоятельно, а использует ту, которую определил обучающий их вышестоящий начальник. Знание командиром бригады боевой задачи по предназначению и его опыт позволяют не просто максимально приблизить условия решения учебно-боевой задачи (проведения занятия) к ситуациям реального боя (с использованием лазерных имитаторов стрельбы и поражения (ЛИСП), устройств, имитирующих звуки боя, визуальные эффекты и т. п.), но и увязать все вопросы, отрабатываемые на учениях и занятиях в рамках ЕКТЗ, с подготовкой к выполнению боевой задачи.

Таким образом, все занятия по тактической подготовке объединяются не только общей тематикой и исходной обстановкой, но и ее главным компонентом — решаемой боевой задачей. Умение действовать в динамике боя является целью отработки всей темы, что дает возможность достичь высокого уровня полевой выучки обучаемых. Мерилом полевой выучки офицеров и органов управления считается результат практического выполнения подразделением (воинской частью, соединением) решения, выработанного командиром (органом управления) и реализуемого на поле боя (пусть даже виртуальном). Следовательно, главным инструментом, обеспечивающим достижение цели подготовки органов управления (штабов), офицеров, подразделений при рациональном использовании отпущенных времени и средств должен стать, на наш взгляд, именно КТТ. Вариант организации боевой подготовки на основе комплексного подхода с применением КТТ представлен на рисунке 1.

Объединение тренажерных средств различных уровней в целостный комплекс, функционирующий в едином информационном пространстве с применением новых технологий, в том числе ИИ, в перспективе позволит рассматривать создание КТТ как магистральное направление развития всей системы УТС СВ[4]. Одно из базовых требований к перспективному КТТ заключается в необходимости его построения с обязательным использованием средств и возможностей автоматизированной системы управления тактического звена (АСУ ТЗ).

Особое значение в ходе обучения БТГр на КТТ приобретает практическая отработка вопросов комплексного огневого поражения противника в рамках цикла управления разведывательно-огневыми контурами по принципу «разведка—решение—поражение». Эту возможность АСУ ТЗ обеспечивает за счет интеграции в ней средств разведки, управления и поражения[5].

Применение в КТТ средств и технологий из состава АСУ ТЗ позволит готовить командиров подразделений и органы управления с применением тех же средств автоматизации, которые являются в ней штатными, что даст возможность получить двойной эффект. Во-первых, должностные лица с опережением, еще до получения штатных средств АСУ приобретут необходимые навыки в работе на средствах автоматизации. Во-вторых, это позволит существенно сэкономить ресурс штатной АСУ (рис. 2).

Важнейшим условием успешного внедрения КТТ является, на наш взгляд, возможность его встраивания в существующую систему бое-

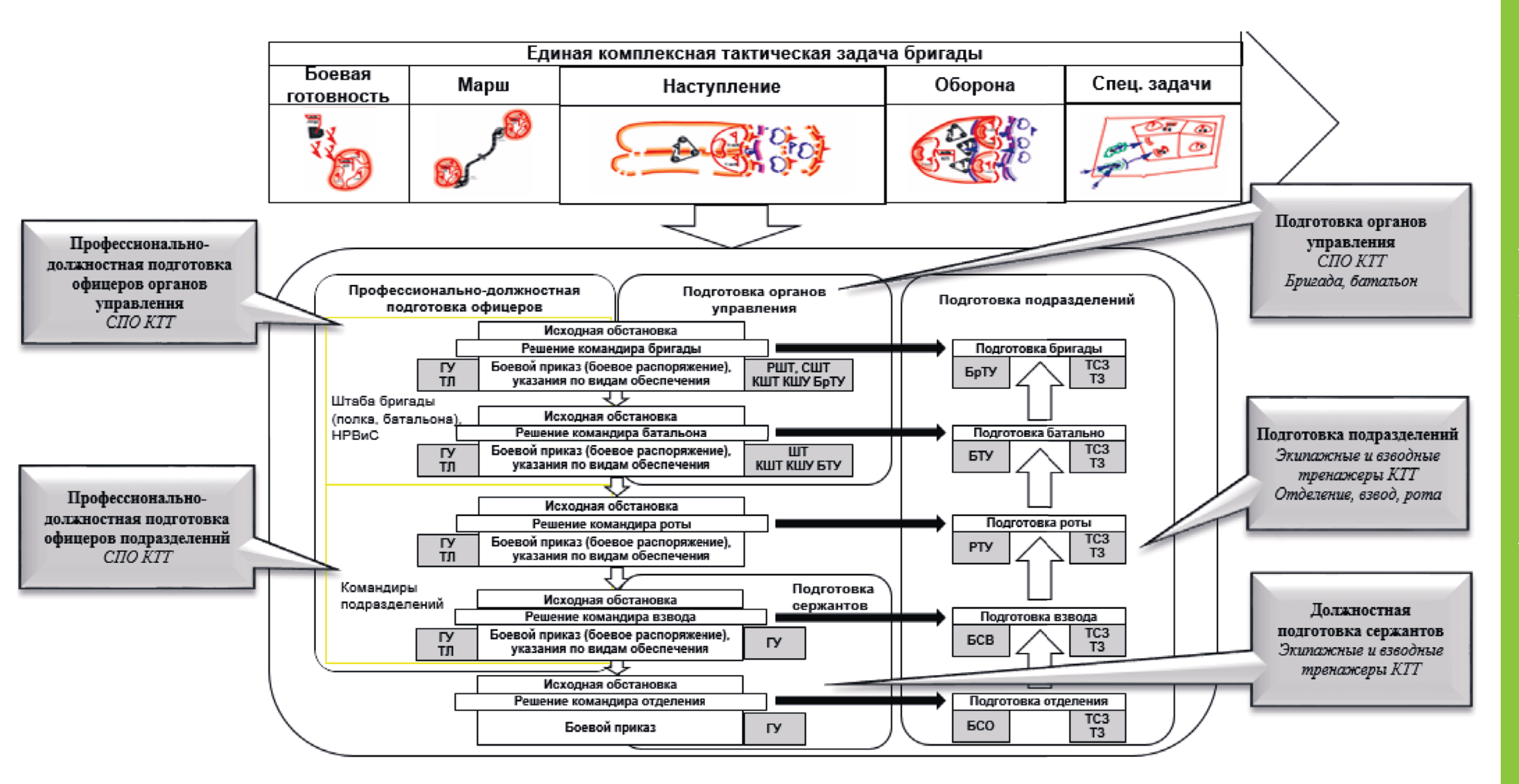
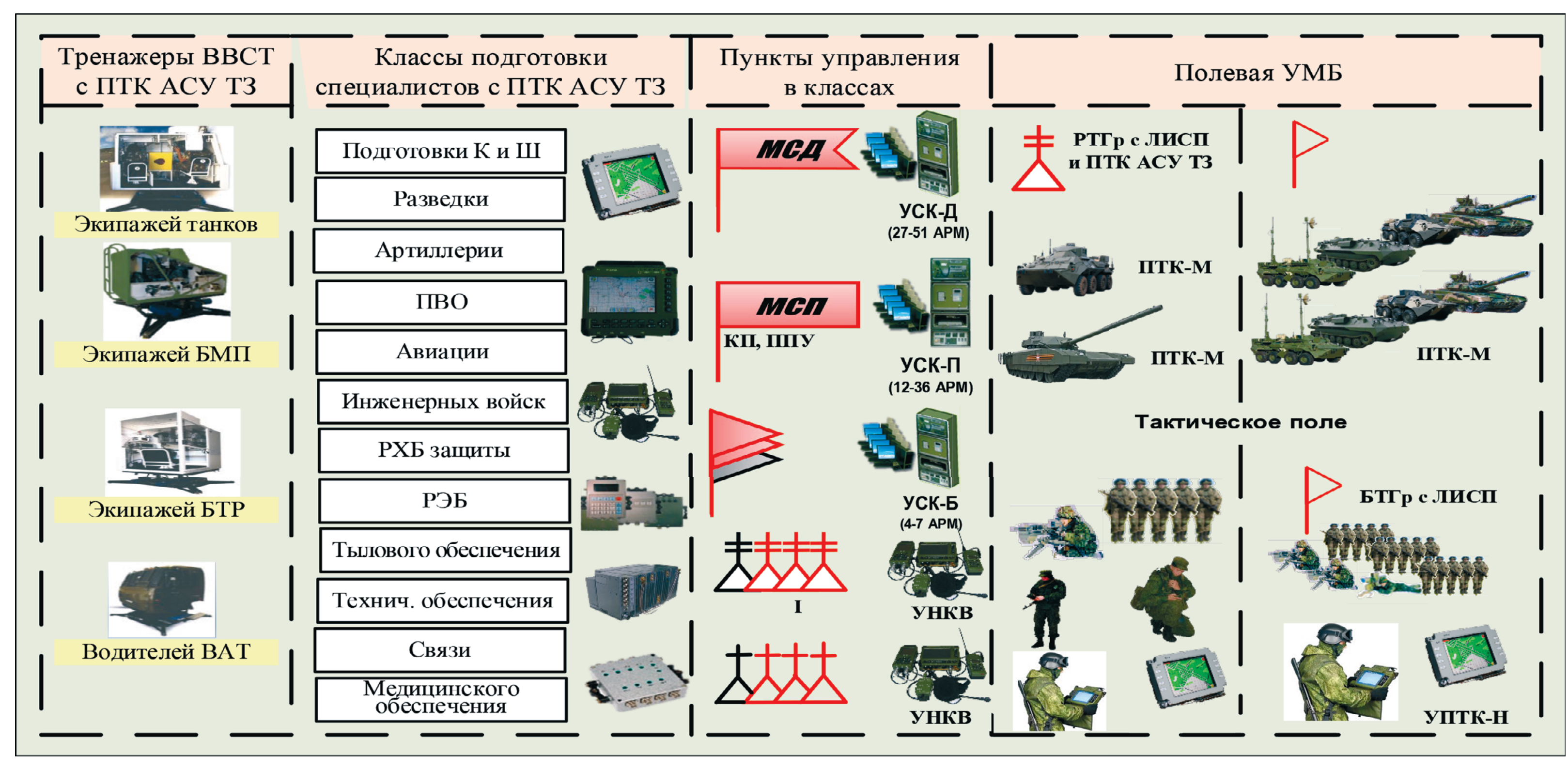


Рис. 1. Комплексный подход к организации подготовки органов управления, офицеров, подразделений с использованием КТТ (вариант)



Примечание: ПТК-М (Н) — программно-технический комплекс мобильный (носимый);
УСК-Д (П, Б) — унифицированный стационарный комплект дивизионный (полковой, батальонный);
УНКВ — универсальный носимый комплект военнослужащего.

Рис. 2. Слаживание органов управления и подразделений с использованием средств АСУ ТЗ на примере центра боевой подготовки (вариант)

вой подготовки и использования в центрах боевой подготовки, в том числе мобильных[6], а также в пунктах постоянной дислокации воинских частей. Следовательно, применение КТТ должно обеспечить органичное сочетание традиционных форм и методов подготовки с компьютерными технологиями и технологиями ИИ, что позволит вывести процесс боевой учебы на новый, интеллектуальный уровень.

Встраиваемость КТТ в существующую организацию боевой подготовки достигается планированием мероприятий профессионально-должностной подготовки офицеров, слаживания органов управления и подразделений в соответствии с разработанной ЕКТЗ, где каждый отрабатываемый вид боя (тактического действия) сгруппирован в модуль. В рамках модуля взаимоувязаны и согласованы (на основе решения командира) все формы подготовки офицеров и органов управления с боевой учебой подразделений (рис. 3).

При этом чередование занятий с использованием КТТ и занятий на полевой УМБ обеспечивает реализацию основополагающего принципа обучения — «от простого к сложному». Занятия на тренажере позволят добиться устойчивых навыков в управлении экипажем, расчетом и подразделением до перехода на материальную часть с расходом моторесурсов, боеприпасов, горюче-смазочных материалов и других материальных средств[7].

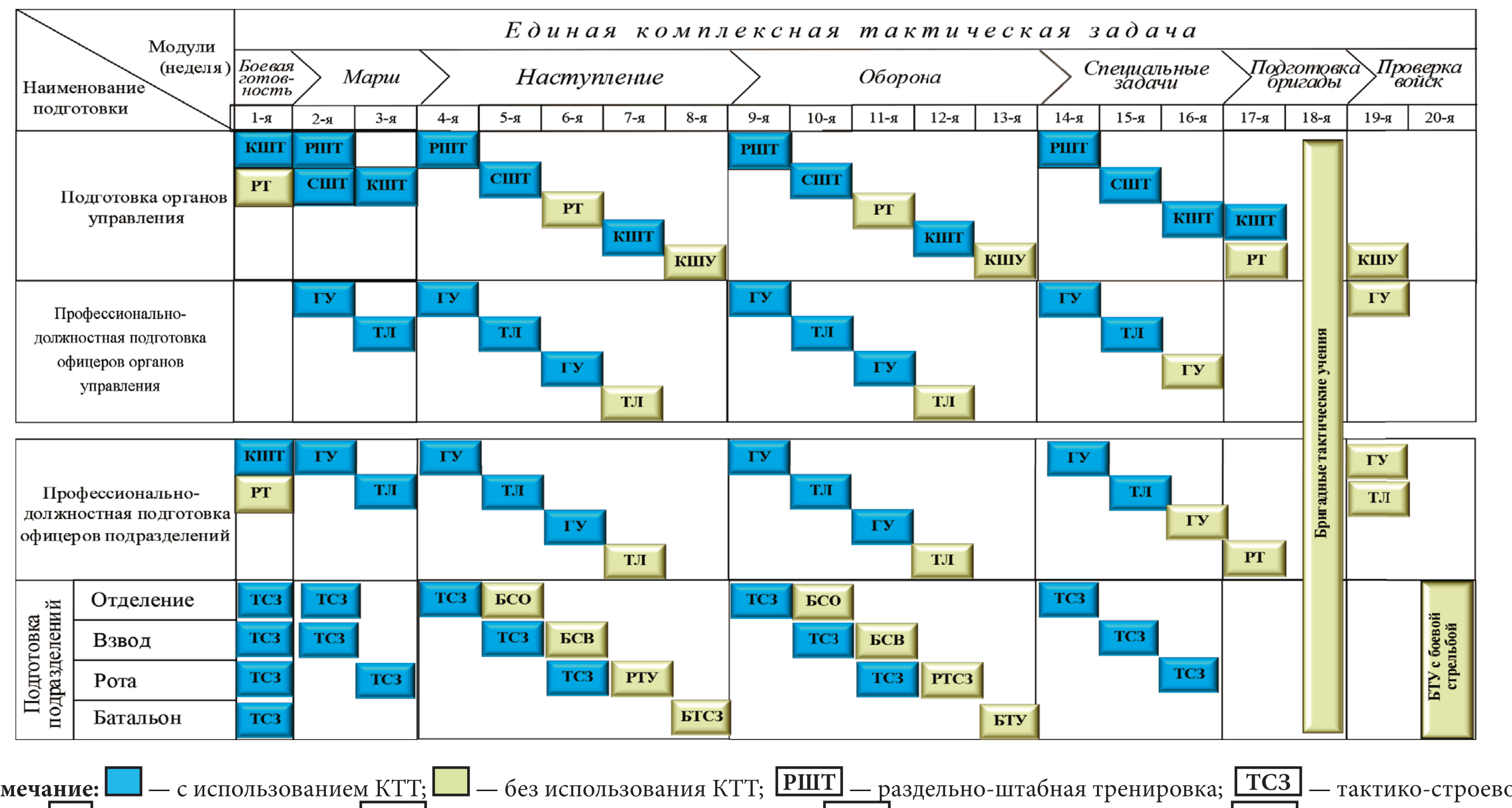
Приведенный на рисунке 3 вариант планирования мероприятий боевой подготовки на основе комплексного подхода позволяет, на наш взгляд, эффективно готовить соединения и воинские части к предстоящим действиям независимо от территориального расположения объектов полевой УМБ относительно пунктов постоянной дислокации.

Применение КТТ в условиях комплексного подхода будет наиболее плодотворным при использовании новых программ боевой подготовки (2017—2019 годов издания), в основе которых лежит «модульный» принцип слаживания подразделений.

Содержание модуля соответствует одному виду боевых действий и одному конкретному способу выполнения задачи. Темы предметов боевой подготовки, формирующих понятие «полевая выучка», выстраиваются вокруг темы тактической подготовки как основы всего модуля. В результате обучение строится на основе принципа «поэтапной» подготовки, а в каждом модуле отрабатывается один вид боевых действий на основе решения старшего начальника на бой (тактическое действие).

Модульная организация боевой подготовки позволит обеспечить более высокий и равномерный рост боеспособности обучаемых подразделений в течение учебного года, сократить сроки их готовности к выполнению боевых задач по предназначению. Проведенные расчеты показывают, что темпы приращения боеспособности мотострелкового батальона (мсб), проходящего подготовку по модульному принципу, в 1,5—2 раза выше, чем при поэтапном боевом слаживании (рис. 4).

Объединение тренажерных средств различных уровней в целостный комплекс, функционирующий в едином информационном пространстве с применением новых технологий, в том числе искусственного интеллекта, в перспективе позволит рассматривать создание комплексных тактических тренажеров как магистральное направление развития всей системы учебно-тренировочных средств Сухопутных войск.



Примечание: [синий] — с использованием КТТ; [светлый] — без использования КТТ; РШТ — раздельно-штабная тренировка; ТСЗ — тактико-строевое занятие; ТЗ — тактическое занятие; СШТ — совместная штабная тренировка; БСО — боевая стрельба отделения, БСВ — боевая стрельба взвода, РТУ — ротное тактическое учение, БТУ — батальонное тактическое учение, БТСЗ — батальонное тактико-специальное занятие; КШУ (Т) — командно-штабное учение (тренировка).

Рис. 3. Планирование подготовки офицеров, органов управления и подразделений с использованием КТТ (вариант)

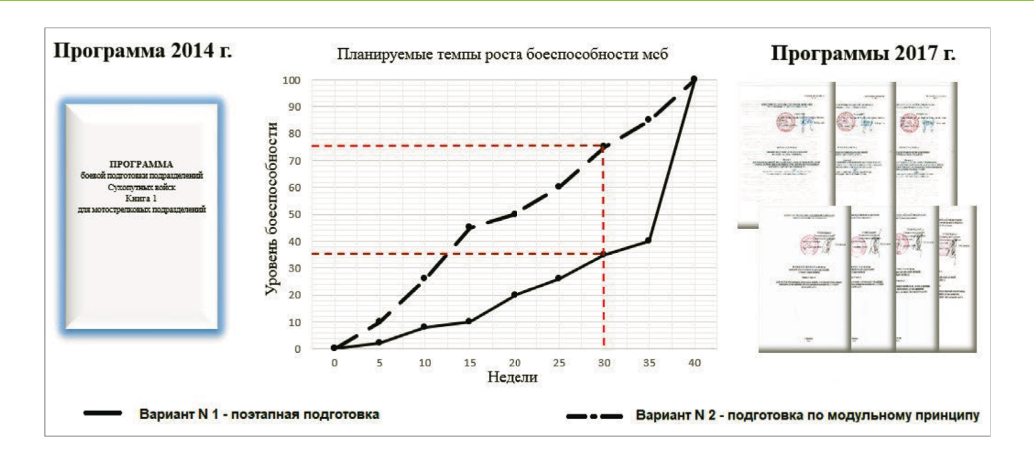


Рис. 4. Сравнение темпов приращения боеспособности мсб, проходящего поэтапную подготовку и обучение по модульному принципу

Таким образом, боевая подготовка, организованная на основе новых программ боевой подготовки в сочетании с применением перспективных УТС, главным из которых является КТТ, может обеспечить существенный рост уровня обученности подразделений и органов управления общевойсковых формирований тактического звена СВ типа БТГр. Такой подход будет в полной мере соответствовать обозначенным приоритетам боевой учебы СВ, цель которых — повышение качества проведения мероприятий боевой подготовки, совершенствование слаженности органов управления и подразделений различного уровня на основе современных информационных и дидактических технологий.

Необходимо отметить, что в дальнейшем процесс создания, внедрения КТТ и его опытной эксплуатации потребует проведения научных исследований для решения ряда проблемных вопросов. В частности, необходимо определить дополнительные требования к структуре, составу, дидактическим и техническим характеристикам КТТ, разработать методики оценки эффективности боевой подготовки и ее приращения за счет внедрения КТТ, провести эксперимент, выработать рекомендации по его применению и, наконец, подготовить предложения по внесению изменений в руководящие документы, регламентирующие организацию боевой подготовки.

ПРИМЕЧАНИЯ

[1] Наставление по боевой подготовке в Вооруженных Силах Российской Федерации. М.: Воениздат, 2013. 167 с.

[2] Там же.

[3] Там же.

[4] Концепция развития учебно-тренировочных средств (тренажеров) Вооруженных Сил РФ до 2027 года, утвержденная приказом Министра обороны РФ от 6 июня 2019 года. М.: МО РФ, 2019. 48 с.

[5] *Владимиров И.В., Хватов Ф.Ю., Якимов В.Н.* Роль и место АСУ ТЗ в системе боевой подготовки Сухопутных войск // Вестник Академии военных наук. 2021. № 3. С. 86—91.

[6] Концепция развития межвидовых мобильных центров боевой подготовки. Проект. М.: ВУНЦ СВ «Общевойсковая академия ВС РФ», 2018. 161 с.

[7] *Владимиров И.В., Хватов Ф.Ю. Якимов В.Н.* Роль и место АСУ ТЗ...

Наращивание иностранными государствами возможностей ведения противоборства в киберпространстве

Полковник М.П. СИДОРОВ

Майор С.Н. ОВСЯННИКОВ

АННОТАЦИЯ

Авторами поставлена цель ознакомить аудиторию с понятием киберпространство, показать отводимую ему роль и значимость для достижения геополитических целей и решения военно-политических задач. На примере США и коллективного Запада обозначены узловые элементы формирования системы кибербезопасности, в качестве подтверждения масштабов развития кибервойск приведены факты финансирования их развития, также освещены вопросы подготовки киберспециалистов и специфика проводимых киберучений.

ABSTRACT

The authors set themselves the goal of acquainting the reader with the concept cyberspace, showing the role reserved for it, and its significance in attaining geopolitical objectives and solving military-political problems. They turn to the practices of the United States and collective West to exemplify the nodular elements of forming the system of cyber security citing facts of their development funding to confirm the scale of cyber troops progress, and also highlighting issues of training cyber experts and specific features of cyber exercises.

КЛЮЧЕВЫЕ СЛОВА

Киберпространство, система кибербезопасности, киберучения.

KEYWORDS

Cyberspace, system of cyber security, cyber exercises.

ИНТЕРНЕТ, изначально разрабатываемый в качестве среды передачи информации военного назначения, стал фундаментом формирования нового измерения, виртуальной среды — кибернетического пространства. «Киберпространство» — это глобальное пространство в цифровой среде, состоящее из взаимозависимых сетей информационно-коммуникационных инфраструктур, в том числе Интернета, сетей связи, компьютерных сетей, встраиваемых процессоров и контроллеров[1].

Широкие информационно-технологические возможности киберпространства используются не только для достижения мирных целей. Посредством целенаправленного воздействия на социум и объекты инфраструктуры разрешаются межгосударственные противоречия, решаются военно-политические и иные задачи, в том числе — в ущерб международной безопасности и стратегической стабильности. Для этого задействуется как оборонительный, так и наступательный киберпотенциал.

Традиционные средства ведения войны активно дополняются гибридными воздействиями, будь то изменение управляющего техническими ресурсами программного кода, кража, подмена или уничтожение важнейших данных, прогнозируемое изменение сознания населения или индивида, либо управление беспилотными роботизированными аппаратами.

Учитывая широкое проникновение киберсегмента во все сферы деятельности современных государств и общества, США и их западные союзники развивают наступательные возможности в киберпространстве.

Еще в 2003 году в «Национальной стратегии по защите киберпространства» был предложен интегрированный подход к обеспечению кибербезопасности, в рамках которого назначено координирующее ведомство — министерство внутренней безопасности США (рис. 1).

Рис. 1. Эмблема министерства внутренней безопасности США

В целях повышения эффективности системы и развития ее компонентов в 2009 году руководство системой кибербезопасности было передано министерству обороны Соединенных Штатов.

В том же году был разработан и утвержден ряд документов, закрепивших основы проведения оборонительных и наступательных операций в киберпространстве. Понимание необходимости централизованного управления разрозненными киберподразделениями привело к созданию Командования боевых действий в кибернетическом пространстве в составе объединенного стратегического командования вооруженных сил США (Киберком) со штатной численностью более 60 тыс. человек (рис. 2).

К компонентам видов вооруженных сил США, находящимся в опе-

Рис. 2. Эмблема Киберкома США

ративном подчинении Киберкома, относятся: четыре командования боевых действий в кибернетическом пространстве (сухопутных войск, военно-морских сил, морской пехоты, береговой охраны) и 24-я воздушная армия (боевых действий в кибернетическом пространстве) военно-воздушных сил США.

В 2018 году на основе Киберкомандования сформированы силы кибероперируций, объединившие состав вооруженных сил страны и органов государственного управления, придав командованию значение отдельного вида вооруженных сил и значительно расширив его возможности и полномочия[2].

В том же году созданное Агентство кибербезопасности и безопасности инфраструктуры (*Cybersecurity and Infrastructure Security Agency, CISA*) Министерства внутренней безопасности США объединило основные организации, в компетенцию которых входит защита критически важных объектов на территории США и их союзников (рис. 3). В его состав вошли три департамента по направлениям: кибербезопасность, безопасность инфраструктуры и коммуникации в условиях чрезвычайных ситуаций.

С формированием *CISA* значительно расширились полномочия Министерства внутренней безопасности (в обход судебных процедур), что позволило более активно привлекать к установлению источников угроз национальной безопасности в киберпространстве Агентство национальной безопасности, Федеральное бюро расследований, Центральное разведывательное управление, Государственный департамент, подконтрольные СМИ, крупные IT-компании, научные, образовательные и культурные организации.

В 2018 году кардинально пересмотрены взгляды США на использование киберпространства, определившие его роль в достижении геополитических целей. При непосредственном участии Д. Трампа были разработаны следующие документы: «Национальная киберстратегия США», «Киберстратегия министерства обороны США», Стратегия объединенного киберкомандования вооруженных сил США «Завоевание и удержание превосходства в киберпространстве».

**Рис. 3. Эмблема
Агентства кибербезопасности
и безопасности инфраструктуры**

В соответствии с положениями этих документов, Россия, Иран и Северная Корея рассматриваются как противники и киберпреступники, которые должны заплатить «цену,

достаточную для сдерживания подобных агрессивных действий в будущем», а Китай открыто обвиняется в экономическом шпионаже. Также указано, что «Россия, Китай, Иран и Северная Корея используют киберпространство в качестве площадки для противостояния Соединенным Штатам, их союзникам и партнерам, зачастую с безрассудством, на которое они не могли бы рассчитывать в любой другой среде». В разделе «Поддержание мира с использованием силы» в качестве цели указано «сохранение превосходства Соединенных Штатов в киберпространстве и применение его возможностей для обеспечения господства в других средах»[3].

При этом киберпространство рассматривается как новая сфера вооруженной борьбы — область боевых действий наравне с воздухом, сушей, морем и космосом. Указано, что реализация национальных интересов США должна обеспечиваться доминированием в информационной сфере в глобальных масштабах и в киберпространстве в частности.

Анализ документов показывает, что идеологический курс американского руководства направлен на насаждение прав США и их союзников на глобальное доминирование, в том числе в мировом информационном пространстве, при посягательстве на которые якобы будут нарушены демократические ценности, за что неминуемо последует наказание «провинившихся» государств.

Соединенными Штатами последовательно реализуются положения вышеописанной национальной киберстратегии. Проводятся внутренние организационные мероприятия по формированию единой системы обеспечения национальной кибербезопасности. В целях совершенствования организационно-штатной структуры Киберкомандования США в качестве основных его сил рассмотрены 12 подразделений из состава 915-го батальона обеспечения киберопераций. В конце 2021 года в его состав вошло первое управление информационных операций, что повысило оперативность принятия решений на применение сил и средств для действий в киберпространстве.

В 2021 году создан новый штаб Киберкомандования США «Фортитьюд Холл» (форт Гордон, штат Джорджия), оснащенный новейшим высокотехнологичным оборудованием. На его создание было потрачено более 360 млн долл.[4]

Для перевода системы кибербезопасности страны на единую унифицированную платформу разработана «Единая архитектура боевых действий в киберпространстве» (*The Joint Cyber Warfighting Architecture)*, позволяющая осуществлять взаимодействие всех компонентов киберобороны США с использованием единых стандартов, что повысило оперативность управления и эффективность проводимых мероприятий[5].

Наряду с этим запущен проект «Ай-Кей-И» (*Project IKE*), позволяющий осуществлять моделирование киберопераций и оценивать последствия их проведения с использованием технологий искусственного интеллекта. Стоит отметить, что американская «Стратегия использования искусственного интеллекта в аппаратных средствах» предполагает автоматизацию контроля всех существующих процессов, построенных на основе нейросетевых алгоритмов[6].

Большое внимание уделяется подготовке кибер-специалистов. Так, в 2020 году разработана учебная платформа «Устойчивая среда для кибертренинга» (*The Persistent Cyber Training Environment*), позволяющая проводить учебно-боевые занятия по киберподготовке между географически удаленными подразделениями[7].

Отдельного внимания заслуживают объемы финансирования Соединенными Штатами программ по поддержанию и развитию сил и средств противоборства в информационном пространстве.

Так, сенат конгресса США одобрил законопроект об оборонном бюджете на 2022 год объемом 768 млрд долл. — часть средств будет направлена на усиление кибербезопасности Соединенных Штатов[8].

Значительные суммы (более 3,528 млрд долл.) идут на проведение перспективных разработок Агентством перспективных исследовательских проектов США (*Defense Advanced Research Projects Agency, DARPA*) (рис. 4). Данная организация отвечает за разработку новых технологий в интересах вооруженных сил. Ключевой задачей *DARPA* является сохранение технологического превосходства вооруженных сил США, а также предотвращение внезапного для США появления новых технических средств вооруженной борьбы и поддержка прорывных исследований. Направлениями деятельности агентства являются: адаптивное управление, оборонные исследования, инновации в информационных, микросистемных, стратегических и биологических технологиях. На особом контроле *DARPA* находится развитие технологий в области противодействия кибертерроризму[9].

Рис. 4. Эмблема Агентства перспективных исследовательских проектов США

DARPA разрабатывает решения по общесистемному администрированию многодоменных сетей. В течение двух лет планируется освоить до 20 млн долл. для разработки системы автономного обнаружения и настройки взаимосвязанных компонентов сетей военного назначения в режиме реального времени.

Данные мероприятия выполняются в рамках общей программы «Комплексный контроль сетей» (*Mission-Integrated Network Control*), направленной на разработку системы достоверной и своевременной передачи критически важной информации в динамически изменяемых сетях, основанных на гетерогенных вычислительных системах[10].

Хакерские атаки на энергетическую инфраструктуру США в 2021 году инициировали принятие дополнительного пакета мер по модернизации системы информационной безопасности критически важных объектов страны. Общий объем выделенных средств составил более триллиона долларов.

Для работы в «серой зоне», находящейся вне пределов международной правовой юрисдикции, конгресс США регулярно выделяет десятки миллионов долларов на создание так называемого теневого Интернета и оказание помощи оппозиции в различных государствах при проведении цветных революций.

Таким образом, расходы Соединенных Штатов только на поддержание и развитие сил и средств противоборства в информационном пространстве имеют тенденцию к увеличению, а в абсолютном значении многократно превосходят бюджеты некоторых стран мира.

Вашингтон, развивая национальные кибервозможности, демонстрирует стремление взять под контроль соответствующие структуры своих союзников в Европе. В подтверж-

дение данного тезиса в национальной киберстратегии США указано, что «повышение киберпотенциала стран-партнеров способствует обеспечению их защиты, повышает возможности этих государств по оказанию помощи Вашингтону в противодействии общим угрозам, а также решению более обширного спектра задач в сферах дипломатии, экономики и безопасности»[11].

Американское руководство продолжает политику объединения потенциала сил и средств в киберпространстве за счет наращивания взаимодействия с партнерами по НАТО. В 2002 году руководство Североатлантического альянса в ходе Пражского саммита впервые включило в повестку вопросы строительства единой системы кибероброны, а на Рижском саммите в 2006 году лидеры стран НАТО подтвердили необходимость обеспечения дополнительной защиты своих информационных систем.

При этом руководство альянса, выделяя кибербезопасность в качестве одного из наиболее приоритетных направлений совершенствования своего оборонительного и наступательного потенциала, по подобию киберкома на территории стран-союзников, в том числе потенциальных членов НАТО, создает единую межгосударственную высокотехнологичную систему кибероброны.

В мае 2008 года семь государств — членов Североатлантического союза (Германия, Испания, Италия, Латвия, Литва, Словакия, Эстония) и Стратегическое командование реформирования объединенных сил НАТО подписали документы о создании в Таллине (Эстония) Центра НАТО по сотрудничеству в сфере кибероброны (Центра передового опыта в области киберзащиты) (*NATO Cooperative Cyber Defence Centre of Excellence, CCD COE*). В том же году центр получил статус Международной военной организации, осуществляющей обмен актуальной информацией о современных угрозах в киберпространстве и способах их нейтрализации (рис. 5).

Рис. 5. Эмблема Центра НАТО по сотрудничеству в сфере кибероброны

В настоящее время членство в этой организации открыто для всех участников Североатлантического альянса. Центр также устанавливает отношения сотрудничества как с государствами, не входящими в НАТО, так и с отдельными университетами, научно-исследовательскими институтами и заинтересованными организациями. По состоянию на февраль 2022 года в CCD COE входят 25 членов НАТО, называемых странами-спонсорами[12].

Центр НАТО по сотрудничеству в сфере кибероброны в настоящее время проводит поиск новых способов защиты информации, занимается развитием единой концепции обеспечения безопасности в киберпространстве, а также координацией действий при проведении наступательных и оборонительных кибероперации.

Основными направлениями исследований, проводимых центром, являются: развитие концепций и стратегий обеспечения безопасности

в киберпространстве, разработка технических решений обеспечения безопасности цифровых вычислительных систем, оценка рисков кибератак, моделирование и проведение учений и тренировок в сфере киберзащиты стран — участниц альянса.

Еще в июне 2021 года североатлантический альянс признал кардинальные изменения ландшафта угроз и необходимость учитывать в своей деятельности трансформацию киберпространства. Это обусловило принятие новой всеобъемлющей политики киберзащиты для решения трех основных задач НАТО — коллективной обороны, кризисного управления и безопасности на основе сотрудничества. По ее замыслу киберпотенциал Североатлантического альянса должен обеспечить сдерживание, защиту и противодействие всему спектру киберугроз как в мирное, так и в военное время, а также при разрешении кризисных ситуаций во всех сферах: политической, военной и технической[13]. В рамках поддержания на требуемом уровне способности оперативного реагирования на угрозы информационной безопасности расширяется программа подготовки профильных специалистов. Так, под общим руководством представителей Центра передового опыта НАТО в области киберзащиты на 2022 год запланированы порядка 20 курсов как в очном, так и в онлайн режиме, девять мобильных курсов, несколько курсов электронного обучения, два киберучения, ряд практических семинаров и ежегодная конференция[14].

Одним из основных и активных участников центра является Германия. В соответствии с ее доктринальными документами, определяющими политику в сфере национальной обороны, информационное пространство является новой средой ведения боевых действий.

В целях формирования органов, способных эффективно вести оборонительные и наступательные операции в информационном пространстве, командование бундесвера с 2017 года активно развивает новый межвидовой компонент вооруженных сил — Силы кибеопераций и информационного обеспечения (СКИО). Его структура представлена на рисунке 6. В апреле этого же года в качестве шестого по счету высшего органа военного управления в составе вооруженных сил Германии создано Главное командование сил кибеопераций и информационного обеспечения.

Первоначально предполагалось, что на СКИО будут возложены задачи исключительно в сфере обеспечения национальной кибербезопасности, защиты государственных информационных ресурсов, объектов критической инфраструктуры от

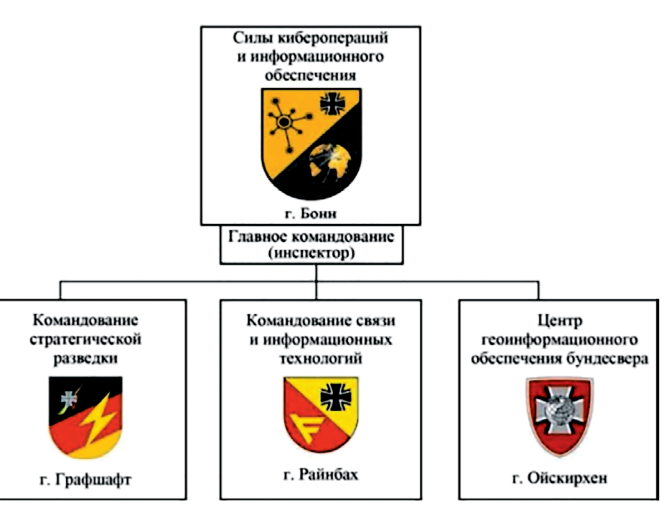


Рис. 6. Структура сил кибеопераций и информационного обеспечения ВС Германии

несанкционированного электромагнитного проникновения. В процессе развития в его состав вошли подразделения радиотехнической разведки и радиоэлектронной борьбы, ранее входившие в состав объединенных сил обеспечения[15].

По инициативе США на базе 24-го батальона 66-й бригады военной разведки сухопутных войск США (Висбаден) в Германии сформирован многонациональный отряд *Northern Raven* для сбора и анализа данных из открытых источников информации. В его состав входят специалисты из США, Великобритании, Литвы, Польши и Эстонии[16].

Вместе с этим Великобритания ведет курс на развитие собственных сил, способных отстаивать национальные интересы в киберпространстве.

В 2019 году консервативная партия предложила создать специальную национальную группу по борьбе с киберпреступностью в целях изменения существующего подхода правоохранительных органов Великобритании к кибербезопасности[17]. В этом же году были созданы Национальные киберсилы (*National Cyber Force*) посредством консолидации подразделений кибероброны и подразделений, участвующих в наступательных операциях против кибертерроризма и попыток вмешательства во внутриполитические процессы Соединенного Королевства (рис. 7)[18]. Для

Рис. 7. Слайд доклада армии США о результатах работы отряда *Northern Raven*

этих целей британское правительство выделило более 75 млн фунтов стерлингов[19].

Национальные киберсилы в едином контуре мониторинга и реагирования на киберинциденты взаимодействуют с Национальным центром кибербезопасности (*National Cyber Security Centre*), деятельность которого носит оборонительный характер и направлена на повышение защиты государственных ведомств, стратегической инфраструктуры и промышленности (рис. 8).

Рис. 8. Эмблема Национального британского центра кибербезопасности

Одновременно с Великобританией наращивает усилия по созданию национальных сил кибербезопасности Польша.

Так, в феврале 2019 года министр национальной обороны Польши утвердил «Концепцию организации и функционирования войск обороны киберпространства». Спустя три года польское правительство объявило о создании нового киберкомпонента «Силы защиты киберпространства» (пол. *Wojska Obrony Cyberprzestrzeni)*, отвечающего за проведение операций в киберпространстве (рис. 9). Главной задачей нового подразделения является управление получением, обработкой и предоставлением разведывательных данных при проведении оборонительных и наступательных операций вооруженных сил Польши и ее союзников[20].

Совместно с активным наращиванием возможностей иностранных государств в киберпространстве проводится совершенствование научно-методической базы и выработ-

Рис. 9. Эмблема польских сил защиты киберпространства

ка концепций дальнейшего развития киберпотенциала.

Анализ руководящих и планирующих документов показывает, что киберпространство воспринимается руководством западных стран как полноценная сфера острой конфронтации между государствами. В качестве примера можно рассмотреть доклад «Будущее киберпространства и гибридных угроз» (*The future of cyberspace and hybrid threats)*, подготовленный Европейским центром передового опыта по противодействию гибридным угрозам в апреле 2021 года. В документе отмечается повышение значения искусственного интеллекта в подрывной деятельности и возрастающей роли киберпространства в условиях кризисных ситуаций, а также увеличение зависимости между политикой и технологиями[21].

Центр анализа европейской политики (*Center for European Policy Analysis*) подготовил документ «Создание общих основ трансатлантической кибербезопасности — балтийский подход» (*Building Common Ground in Transatlantic Cybersecurity — A Baltic Approach*), в котором рекомендует в самые короткие сроки создать национальные советы по кибербезопасности для выполнения критически важных задач в этой области, расширить каналы обмена информацией об угрозах в рамках Совета США-ЕС по торговле и технологиям и объединить гражданский и военный опыт в сфере кибербезопасности путем создания объединенного киберподразделения Евросоюза[22].

Более глобальное и прикладное значение имеет доклад центра передового опыта НАТО в области киберзащиты «Киберугрозы и НАТО 2030» (*Cyber Threats and NATO 2030: Horizon Scanning and Analysis,* рис. 10). В нем детально рассмотрены ответные меры НАТО на действия противников в киберпространстве, применяемые новые технологии, боевые действия в киберсфере, необходимость обмена информацией, анализа киберугроз и проведения учений, а также нормативные и политические меры реагирования на вызовы кибербезопасности[23]. Примечательно, что раздел по обзору перспективных противников НАТО целиком посвящен России.

Результаты такого рода исследований подталкивают ряд стран к переосмыслению основополагающих

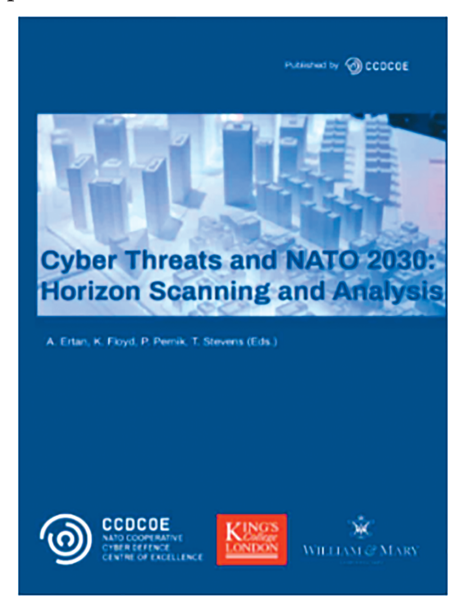


Рис. 10. Доклад «Киберугрозы и НАТО 2030»

Рис. 11. Стратегия кибербезопасности правительства Великобритании

принципов ведения кибервойны. Наиболее серьезные изменения коснулись принципов развития киберпотенциала Соединенного Королевства. Новая стратегия кибербезопасности правительства Великобритании (*Government Cyber Security Strategy*), опубликованная в январе 2022 года (обновлена в феврале 2022 года), рассчитана на 2022—2030 годы и предусматривает форсирование развития интеграционных процессов между бизнесом и правительством (рис. 11). В ближайшей перспективе Лондон намерен создать гарантированно защищенный контур компьютерных сетей для правительственных и силовых структур, а до 2030 года и всей Великобритании. В результате это должно привести к установлению «доминирующей роли Великобритании» в киберпространстве[24].

Согласно «Плану единой сети сухопутных войск США», американским оборонным ведомством предусмотрено проведение комплекса мероприятий по модернизации оборудования, программного обеспечения и сетевой инфраструктуры своих сухопутных войск для обеспечения многосферных операций к 2028 году[25]. Киберцентр передового опыта сухопутных войск США на постоянной основе проводит тренинги с персоналом с целью максимального использования полученного научного и практического опыта при проведении информационных операций по всему миру. Пример обучающего материала представлен на рисунке 12.

В интересах совершенствования навыков личного состава киберподразделений и проведения боевого слаживания странами НАТО на регулярной основе проводятся совместные учения. Наиболее крупным из них стало «Сайбер Коалишн 2021» (*Cyber Coalition* 2021), проведенное в конце 2021 года при непосредственном участии порядка тысячи специалистов киберподразделений Североатлантического альянса и стран — участниц соглашения «Партнерство ради мира» (Ирландии, Финляндии, Швейцарии и Швеции). Цель учения — повышение способности военного альянса противодействовать угрозам в киберпространстве[26].

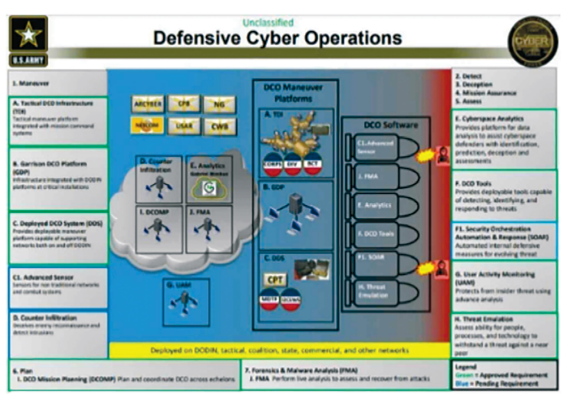


Рис. 12. Презентация армии США по оборонительным действиям в киберпространстве

Кроме учений, при поддержке Центра передового опыта НАТО проводятся ежегодные международные конференции по кибербезопасности, связанные с использованием кибертехнологий в гуманитарной и технической областях.

В рамках научных исследований в области развития средств и способов ведения информационных войн в прошлом году реализован ряд научных работ и исследований, заложивших основу для перспективных разработок.

Так, в 2022 году университетом сил специальных операций ВС США (ССО) спланированы исследования по следующим направлениям: искусственный интеллект и большие данные; поддержка силами ССО протестных движений; Китай, Россия и стратегическое соперничество[27]. Обозначенные области интересов подтверждают смещение фокуса внимания военно-политического руководства США и НАТО с центрально-азиатского и ближневосточного регионов, Афганистана и Ирана, на восток — Российскую Федерацию и Китайскую Народную Республику.

Наращивание зарубежными странами своих возможностей в киберпространстве и реализация масштабных программ по разработке технологий информационного воздействия создают новые вызовы и угрозы национальным интересам Российской Федерации.

Так, для реализации механизмов противодействия России по отстаиванию своих национальных интересов в странах Черноморского бассейна США и НАТО задействуют аналитические центры Восточной Европы.

В отчете румынского аналитического центра (*New Strategy Center*) «Информационное противоборство и информационные операции в Черноморском регионе» (*Information Warfare And Information Operations In The Black Sea Area,* рис. 13) проведена оценка готовности стран региона (Болгарии, Грузии, Молдовы, Румынии, Турции, Украины, Армении и Азербайджана) к отражению киберугроз[28]. В работе даны рекомендации в области государственной политики по повышению устойчивости государственных и частных кибернетических инфраструктур, а также устойчивости цифровой коммуникационной системы к информационным операциям, проводимым противником.

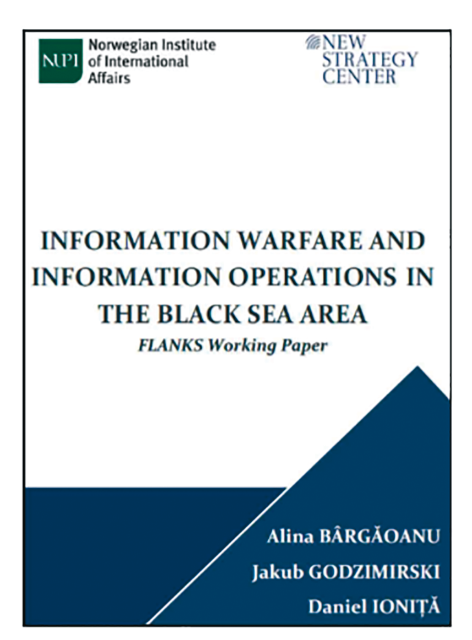


Рис. 13. Отчет «Информационное противоборство и информационные операции в Черноморском регионе»

Еще одним подтверждением рассмотрения России и Китая в качестве информационно-технологических противников США и НАТО является выход в свет книги «Гибридная война: безопасность и асимметричный конфликт в международных отношениях» (*Hybrid Warfare Securityand Asymmetric Conflict in International Relations,* рис. 14)[29]. В ней детально рассмотрены такие вопросы, как: взгляды России на ведение гибридной войны; Китай и его участие в ги-

бридных войнах; гибридная война в странах Балтии. Особое внимание уделено росту уровня напряженности России и Украины. Например, в главе «Дегибридизация: защита Украины от гибридной войны России» авторы обвиняют Москву в проведении информационных кампаний в целях продвижения российских национальных интересов с использованием «серых зон» киберпространства.

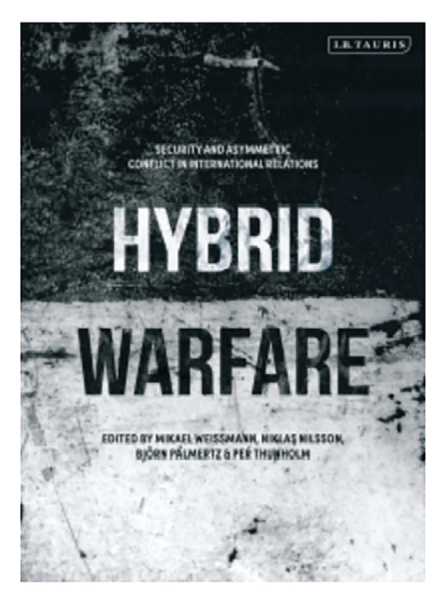


Рис. 14. Книга «Гибридная война: безопасность и асимметричный конфликт в международных отношениях»

Под предлогом подготовки к вступлению в блок НАТО Киевом проводится ряд организационно-правовых мероприятий. Так, согласно стратегии кибербезопасности Украины от 2020 года, в период до 2025 года спланировано наращивание информационного обмена о киберинцидентах с западными партнерами и вхождение в систему кибербезопасности НАТО в качестве элемента, обеспечивающего информационное противоборство с Россией.

В мае 2021 года президент Украины В. Зеленский заявил о создании кибервойск. Тогда же начал функционировать украинский Центр противодействия дезинформации (ЦПД). В круглосуточном режиме 52 сотрудника центра проводили анализ и мониторинг информационного пространства, состояния информационной безопасности и деятельности Украины в данной сфере.

Одновременно с ЦПД был открыт киберцентр по реагированию на компьютерные чрезвычайные события на Украине — *UA*30. В работе центра принимала участие правительственная команда (*CERT-UA*), взаимодействующая с международным Форумом команд реагирования на инциденты безопасности (*FIRST*)[30].

Также в рамках реализации программы *EU4DigitalUA* в сентябре прошлого года под управлением специалистов «Эстонской академии электронного управления» (*eGA*) и эстонской компании «Сайбэксер технолоджи» (*CybExer Technologies*) с сотрудниками Государственной службы специальной связи и защиты информации Украины, Службы безопасности Украины, Киберполиции, Минобороны и Национального банка Украины проведены масштабные киберучения. Их главной целью было определено создание единого киберполигона между компетентными структурами ЕС и Украины для дальнейшей интеграции в единый контур реагирования на угрозы в киберпространстве[31].

Официально основным направлением программы *EU4DigitalUA* является усиление кибербезопасности и защиты данных. До 2024 года в рамках проекта планировалось освоить порядка 25 млн евро[32].

В последние годы усиливается тенденция по наращиванию североатлантическим альянсом своего киберпотенциала у границ России и на территории других государств бывшего социалистического лагеря.

Так, в 2021 году в Вильнюсе начал работу региональный центр киберне-

тической безопасности, создание которого состоялось в рамках реализации Национальной стратегии кибербезопасности Литвы от 2018 года. К созданию Центра активно привлекались специалисты по кибербезопасности из Соединенных Штатов. На проект было выделено около 7 млн евро из государственного бюджета и бюджета ЕС. В задачи центра входит анализ киберугроз, обмен информацией, разработка рекомендаций по кибербезопасности, противостояние гибридным угрозам, организация учений на критически важной инфраструктуре и проведение научных исследований. Новый центр в Каунасе открыт как подразделение Национального центра кибернетической безопасности при минобороны[33].

К работе центра привлекаются специалисты из Украины и Грузии[34].

Также при министерстве обороны Грузии в 2014 году создано бюро кибербезопасности (рис. 15), которое отвечает за создание и развитие стабильных, эффективных и безопасных информационных и коммуникационных систем для субъектов критической информационной системы минобороны.

Бюро реализует превентивные и ответные меры в случае обнаружения кибератак и инцидентов компьютерной безопасности. Оно определяет

Рис. 15. Эмблема бюро кибербезопасности Грузии

политику информационной безопасности в сфере обороны. Бюро уполномочено разрабатывать концептуальные и нормативные документы и нормативно-правовую базу, обеспечивать соответствие международным стандартам и правовым нормам в области кибербезопасности[35].

Начиная с 2019 года представители бюро принимают участие в учениях по кибербезопасности «Амбер мист» (*Amber Mist*), организуемых вооруженными силами Литвы[36].

Отдельного внимания в контексте данной статьи заслуживает Китайская Народная Республика.

Китай, прочно заняв место регионального лидера в киберпространстве Центральной и Юго-Восточной Азии, стремится к завоеванию господствующего положения в глобальном информационном пространстве.

Начиная с 2016 года правительство КНР выработало новые подходы к модернизации национальной системы обеспечения кибербезопасности. В результате проведения военной реформы создан новый вид вооруженных сил — силы стратегической поддержки Народно-освободительной армии Китая (НОАК). Одной из основных целей деятельности этого вида НОАК является получение превосходства над потенциальными противниками в космическом и киберпространстве.

Значительный интерес для исследователей представляет Национальный центр кибербезопасности Китая (НЦКК), строительство которого ведется с 2017 года. Центр представляет собой грандиозный комплекс, расположенный на участке площадью 40 км кв. в городе Ухань (провинция Хубэй). Официально центр называется Национальная база талантов и инноваций в области кибербезопасности.

НЦКК включает семь центров исследований, развития талантов и предпринимательства, две государственные лаборатории и Нацио-

нальную школу кибербезопасности (рис. 16), работающие в интересах Министерства государственной безопасности, Министерства общественной безопасности и Сил стратегической поддержки.

Центр укрепит возможности Китая, еще больше обострив конкуренцию в киберпространстве.

Основу центра (первый компонент) составляет Национальная школа кибербезопасности, первый выпуск которой ожидается уже в 2022 году.

Второй компонент — центр развития талантов имеет возможность обучать шесть тысяч стажеров в месяц. Вместе оба компонента Центра могут подготовить более 500 тыс. специалистов в течение десяти лет.

Рис. 16. Космический снимок компании Apollo Mapping территории Национальной школы НЦКК

Для координации работы НЦКК Комиссией Коммунистической партии Китая по делам киберпространства был создан комитет для надзора за операциями и политикой центра, предоставив ему прямую связь с Пекином[37].

В современном мире занятие доминирующего положения в кибернетическом пространстве является ключевым элементом реализации национальных интересов каждого из высокоразвитых технологичных государств. Отставание в данной сфере может привести к таким разрушительным последствиям, как поражение объектов критической инфраструктуры, переформатирование национальной идентичности, изменение государственных границ вплоть до полной утраты суверенитета.

Анализ фактов наращивания возможностей государств по ведению противоборства в киберпространстве в условиях расширения НАТО и проведения Белым домом агрессивной политики свидетельствуют о росте угроз национальным интересам Российской Федерации и ее союзников.

При этом необходимо понимать, что «боевые действия» в киберпространстве ведутся непрерывно, нивелируя грань между мирным и военным временем, с применением методов, отличимых от классического трактования ведения войн и часто в обход международного права.

И только принимая активные действия по выявлению и анализу новых вызовов и угроз в киберпространстве, развивая национальный научно-производственный кластер, своевременно вырабатывая меры защиты и демонстрируя возможности по оказанию мощного противодействия, можно сохранить и независимость и целостность Российской Федерации.

ПРИМЕЧАНИЯ

[1] Словарь военных и связанных терминов; изд. министерства обороны США, 31 января 2011 года. С. 92—93.

[2] Germany Considering Missile Defense Shield with Israeli Arrow 3 Missile. URL: http://www.defense-aerospace.com/cgi-

bin/client/modele.pl?shop= dae&modele= release&prod =193296&cat=3 (дата обращения: 02.02.2022).

[3] National cyber strategy of the United States of America. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 02.02.2022).

[4] Army Cyber Pivots To Pacific: Fogarty. URL: https://breakingdefense.com/2021/05/army-cyber-pivots-to-pacific-fogarty/ (дата обращения: 09.02.2022).

[5] Defense Acquisitions: Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance. URL: https://www.gao.gov/products/gao-21-68. (дата обращения: 09.02.2022).

[6] A cyber tool that started at DARPA moves to Cyber Command. URL: https://www.c4isrnet.com/cyber/2021/04/20/a-cyber-tool-that-started-at-darpa-moves-to-cyber-command/ (дата обращения: 09.02.2022).

[7] Cyberwarriors receive updated training tool. URL: https://www.c4isrnet.com/show-reporter/cybercon/2020/10/28/cyberwarriors-receive-updated-training-tool/ (дата обращения: 08.02.2022).

[8] Senate passes 2022 defense authorization bill. URL: https://fcw.com/security/2021/12/senate-passes-2022-defense-authorization-bill/359851/ (дата обращения: 09.02.2022).

[9] U.S. Department of Defense Explores Biotech. URL: https://www.darpa.mil/NewsEvents/Releases/2014/04/01.aspx (дата обращения: 28.02.2022).

[10] DARPA Selects Peraton Labs to Create Multi-Domain Network Orchestration Solution. URL: https://www.prnewswire.com/news-releases/darpa-selects-peraton-labs-to-create-multi-domain-network-orchestration-solution-301476641.html (дата обращения: 09.02.2022).

[11] National cyber strategy of the United States of America. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 08.02.2022).

[12] The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. URL: https://ccdcoe.org/ (дата обращения: 08.02.2022).

[13] Cyber defence NATO. URL: https://www.nato.int/cps /en/natohq/topics_78170.htm (дата обращения: 23.02.2022).

[14] NATO CCDCOE TRAINING CATALOGUE, 2022. URL: http://ccdcoe.org/uploads/2021/12/2022_NATO_CCD_COE_Training_Catalogue_FINAL.pdf (дата обращения: 09.02.2022).

[15] Зарубежное военное обозрение. 2019. № 9. С. 21—25.

[16] Thinking Outside the SCIF: US Army Announces OSINT Journey Moving Forward URL: https://news.clearancejobs.com/2021/04/08/thinking-outside-the-scif-us-army-announces-osint-journey-moving-forward/ (дата обращения: 9.02.2022).

[17] Conservatives propose national cybercrime URL: https://www.computerweekly.com/news/252474489/Conservatives-propose-national-cyber-crime-force (дата обращения: 9.02.2022).

[18] UK to launch specialist cyber force able to target terror groups URL: https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups (дата обращения: 10.02.2022).

[19] UK is nearly ready to launch force to hit hostile countries with cyberattacks URL: https://www.independent.co.uk/news/uk/home-news/cyber-warfare-security-force-iran-crisis-ministry-of-defence-a9278591.html (дата обращения: 10.02.2022).

[20] Thinking Outside the SCIF: US Army Announces OSINT Journey Moving Forward URL: https://news.clearancejobs.com/2021/04/08/thinking-outside-the-scif-us-army-announces-osint-journey-moving-forward/ (дата обращения: 10.02.2022).

[21] Hybrid CoE Trend Report 6: The future of cyberspace and hybrid threats URL: https://www.hybridcoe.fi/publications/hybrid-coe-trend-report-6-the-future-of-cyberspace-and-hybrid-threats/ (дата обращения: 12.02.2022).

[22] Building Common Ground in Transatlantic Cybersecurity – A Baltic URL:

http://cepa.org/building-common-ground-in-transatlantic-cybersecurity-a-baltic-approach/ (дата обращения: 16.02.2022).

[23] Cyber Threats and NATO 2030: Horizon Scanning and Analysis URL: http://kclpure.kcl.ac.uk/portal/files/142284634/Cyber_Threats_and_NATO_2030_Horizon_Scanning_and_Analysis.pdf (дата обращения: 16.02.2022). Unified Network Plan - U.S. Army URL: https://api.army.mil/e2/c/downloads/2021/10/07/d43180cc/army-unified-network-plan-2021.pdf (дата обращения: 18.02.2022).

[24] Government Cyber Security Strategy Building a cyber resilient public sector. URL: https://assets.publishing.service.gov.uk/government/uploads/system/ uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf (дата обращения: 17.02.2022).

[25] Unified Network Plan - U.S. Army. URL: https://api.army.mil/e2/c/downloads/2021/10/07/d43180cc/army-unified-network-plan-2021.pdf (дата обращения: 18.02.2022).

[26] CYBER COALITION 2021 CONCLUDES IN ESTONIA. URL: https://shape.nato.int/news-archive/2021/cyber-coalition-2021-concludes-in-estonia#:~:text=TALLINN%2C%20Estonia%20%2D%20NATO%20concluded%20its,3%2C%202021 (дата обращения: 18.02.2022).

[27] JOINT SPECIAL OPERATIONS UNIVERSITY URL: https://nps.edu/documents/115559645/121916825/2021+Dist+A+JSOU+Special+Operations+Research+Topics+2022.pdf/7858f891-cce7-8e85-f7cb-63f912a1ad0d?version=1.0&t=1626374798838&download=true (дата обращения: 21.02.2022).

[28] INFORMATION WARFARE AND INFORMATION OPERATIONS IN THE BLACK SEA AREA FLANKS Working Paper URL: https://www.newstrategycenter.ro/wp-content/uploads/2019/11/FLANKS-Working-Paper-Information-Warfare-And-Information-Operations-in-the-Black-Sea-Area.pdf (дата обращения: 21.02.2022).

[29] Hybrid Warfare: Security and Asymmetric Conflict in International Relations. URL: https://www.researchgate.net/publication/349497596_Hybrid_Warfare_Security_and_Asymmetric_Conflict_in_International_Relations (дата обращения: 24.02.2022).

[30] В СНБО обсудили создание кибервойск в Украине. URL: https://gordonua.com/news/politics/v-snbo-obsudili-sozdanie-kibervoysk-v-ukraine-kabmin-dolzhen-podgotovit-zakonoproekt-1572134.html (дата обращения: 25.02.2022); EU4DigitalUA. URL: https://eufordigital.eu/ru/discover-eu/eu4digitalua/ (дата обращения: 24.02.2022).

[31] Cyber trainings to enhance Ukraine's skills to respond to cyberattacks. URL: https://ega.ee/news/cyber-trainings-to-enhance-ukraine-s-skills-to-respond-to-cyberattacks/ (дата обращения: 25.02.2022).

[32] EU4DigitalUA. URL: https://eufordigital.eu/ru/discover-eu/eu4digitalua/ (дата обращения: 24.02.2022).

[33] В Литве открылся еще один центр кибербезопасности. URL: https://lt.sputniknews.ru/20210720/v-litve-otkrylsya-esche-odin-tsentr-kiberbezopasnosti-17643313.html (дата обращения: 24.02.2022).

[34] Литва и США строят в Каунасе инфраструктуру для кибернетической войны. URL: https://eadaily.com/ru/news/2019/07/03/litva-i-ssha-stroyat-v-kaunase-infrastrukturu-dlya-kiberneticheskoy-voyny (дата обращения: 25.02.2022).

[35] Cyber Security Bureau. URL: https://mod.gov.ge/en/page/59/cyber-security-bureau (дата обращения: 25.02.2022).

[36] Representatives of Cyber Security Bureau Participate in the Cyber Exercise «Amber Mist 2020». URL: https://mod.gov.ge/en/news/read/7968/representatives-of-cyber-security-bureau-participate-in-the-cyber-exercise-amber-mist-2020%E2%80%9D (дата обращения: 25.02.2022).

[37] China's National Cybersecurity Center A Base for Military-Civil Fusion in the Cyber Domain. URL: https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-National-Cybersecurity-Center.pdf (дата обращения: 25.02.2022).

Развитие теории и практика маскировки в вооруженных силах США

Р.Ю. ГОРОХОВ,
кандидат технических наук

АННОТАЦИЯ

Рассматриваются основные этапы развития маскировки в вооруженных силах США, соответствующий терминологический аппарат и теоретическая база, оценивается опыт скрытия, имитации войск и объектов, дезинформации противника в военных конфликтах последних десятилетий, а также раскрываются современные способы реализации обманных действий.

КЛЮЧЕВЫЕ СЛОВА

Маскировка, скрытие, имитация, дезинформация, обманные действия.

ABSTRACT

The paper examines the chief stages in the progress of camouflage in the US armed forces, the corresponding terminology apparatus and theoretical base, assessing the experience of concealing, simulating troops and facilities, misleading the adversary in military conflicts of the last few decades, and also describing modern decoy methods.

KEYWORDS

Camouflage, concealment, simulation, misinformation, decoy actions.

МАСКИРОВКА как вид боевого обеспечения в вооруженных силах (ВС) США отсутствует. Однако сущность, содержание и направленность мероприятий, реализуемых в целях введения противника в заблуждение относительно истинного состава, возможностей своих войск и планов предстоящих действий, достижения внезапности применения группировок войск (сил) и сохранения их боеспособности, позволяют констатировать логическую и структурно-функциональную тождественность российских и американских подходов к данной деятельности при наличии ряда характерных отличий и особенностей.

Несмотря на то что мероприятия по маскировке войск и объектов в том или ином виде выполнялись практически во всех военных конфликтах с участием ВС США, документальное отображение она получила только в Техническом регламенте *TR 195-45* (1926) и «Инструкции по выполнению инженерных задач в полевых условиях» (1932). Однако изложенные в них рекомендации носили в основном общий описательный характер без конкретных установок по организации маскировки, привлечению сил и средств и расчетов времени на выполнение соответствующих задач, а самое главное — ничего не говорилось о преимуществах, получаемых войсками при качественной

и своевременной реализации мероприятий скрытия и имитации.

К тому же на внедрение маскировки в практику подготовки и ведения боевых действий негативно повлияли скептицизм и непонимание ее важности командным и рядовым составом ВС США. В результате мероприятия скрытия и имитации выполнялись войсками эпизодически и зачастую небрежно. Поэтому **до 40-х годов XX века интенсивность развития маскировки в американских ВС характеризовалась как низкая**[1,2].

Отсутствие должного внимания, глубоких научных изысканий и значительных прорывов в области маскировки было обусловлено еще и тем обстоятельством, что в данный период воинские формирования ВС США вели боевые действия преимущественно наступательного характера. Опора на превосходство в силе как по численности личного состава, так и по качеству вооружения, военной и специальной техники (ВВСТ), а также на результаты заблаговременно предпринимаемых мер по минимизации рисков поражения до начала боестолкновений позволяли пренебрегать мероприятиями маскировки либо выполнять их в ограниченном объеме и масштабе.

Только опыт участия ВС США во Второй мировой войне показал, что вооруженная борьба с хорошо подготовленным, соизмеримым по силе противником, располагающим современными образцами ВВСТ, не может строиться исключительно на принципе наступательности. Достижение победы в сжатые сроки становилось сложной задачей. Массированное применение войск нередко приводило к высоким потерям и не приносило ожидаемого результата, а игнорирование мероприятий пассивной обороны (маскировки) ставило под угрозу безопасность и живучесть важных объектов инфраструктуры на своей территории[3].

В результате отношение к маскировке в ВС США начало меняться в лучшую сторону. На основе тщательного изучения британского опыта защиты военных объектов от ударов германской авиации и оценки катастрофических последствий атак воздушных и подводных сил японского флота на американскую военно-морскую базу Перл-Харбор были инициированы работы в области скрытия важных военных производственных центров на территории США. Так, объекты авиационной промышленности (главное предприятие авиастроительной корпорации Локхид и авиазаводы компаний Дуглас и Боинг) маскировались под кварталы городской застройки с соответствующими атрибутами — дорогами, домами, деревьями и кустарниками (рис. 1)[4].

После проведения данного эксперимента стало очевидно, что комплекс мер по скрытию и имитации, демонстративным (отвлекающим) действиям и дезинформации позволяет существенно снизить потери своих войск (объектов), повысить их живучесть и сохранить боеспособность для нанесения решающих

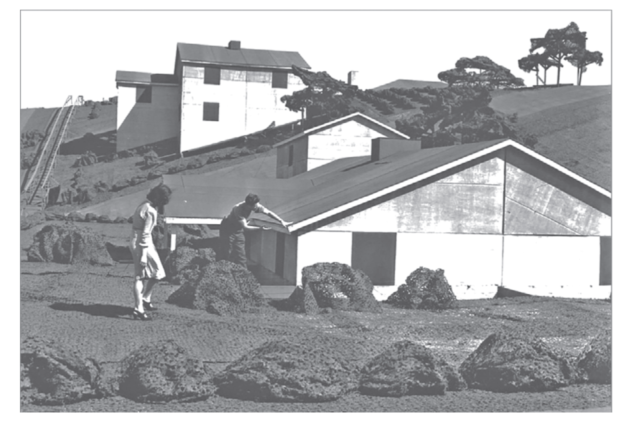


Рис. 1. Скрытие завода под маской-перекрытием в годы Второй мировой войны

ударов по «уязвимым и критически важным точкам» противника. Именно это послужило началом развития маскировки в ВС США как совокупности действий, направленных на сохранение своих войск, достижение победы с минимальными затратами ресурсов и времени.

С 1944 по 1947 год в министерстве обороны США разрабатываются новые подходы к скрытию войск и объектов, нашедшие отражение в следующих уставах:

• *FM 5-20* «Скрытие, основные принципы»;

• *FM 5-20A* «Скрытие личного состава и вооружения»;

• *FM 5-20B* «Скрытие военной техники»;

• *FM 5-20C* «Скрытие районов размещения войск, командных пунктов, пунктов снабжения и медицинских сооружений»;

• *FM 5-20D* «Скрытие позиций полевой артиллерии»;

• *FM 5-20E* «Скрытие авиационной техники на стоянках и аэродромов»;

• *FM 5-20F* «Скрытие средств и позиций ПВО»;

• *FM 5-20G* «Скрытие районов размещения объектов тыла и оборудования фортификационных сооружений»;

• *FM 5-20H* «Средства и приемы скрытия».

По мнению ряда военных специалистов, именно с этого момента в ВС США маскировка приобретает статус раздела военной науки, имеющего как теоретическую, так и прикладную значимость. Научное обоснование получил широкий спектр вопросов, от скрытия одиночного военнослужащего до элементов боевого порядка. Были предложены технические решения для разработки маскировочных комплектов и их распятнения, средств и приемов скрытия демаскирующих признаков деятельности войск, деформирующего трехцветного окрашивания ВВСТ. Выработаны четкие пошаговые инструкции по планированию и контролю выполнения мероприятий маскировки. К решению задач скрытия привлекались преимущественно подразделения инженерных войск[5].

Наряду с этим получила широкое распространение имитация как элемент маскировки. В интересах систематизации информации и формирования четких практических рекомендаций в октябре 1956 года издается ***устав FM 5-23 «Имитация войск и объектов»***. В нем подробно описывались каналы и средства получения разведывательной информации, основные демаскирующие признаки ВВСТ и военных объектов. Текстуально и графически отображался порядок изготовления макетов ВВСТ, элементов оборудования ложных полевых аэродромов, позиций артиллерии, фортификационных сооружений и пунктов полевого водообеспечения. Определялись содержание и способы имитации разрушенных объектов (железнодорожных станций, заводов, мостов и др.), использования дымов, а также особенности имитационных действий в ночное время[6].

В связи с накоплением и систематизацией результатов практического выполнения задач маскировки, а также появлением у противника новых технических средств разведки, работающих в оптическом, тепловом и радиодиапазонах, потребовалась корректировка некоторых положений уставных документов. Так, в январе 1959 года издан переработанный ***устав FM 5-20 «Основные принципы скрытия и их воплощение в бою»***, объединивший в себе практически все направления тактической маскировки. В нем излагались физические основы обнаружения и скрытия объектов, способы и приемы маскировки, специфика выполнения задач

в особых условиях (джунгли, пустыня, заснеженные низкотемпературные географические зоны и др.), порядок использования естественных и искусственных материалов, технических средств маскировки войскового и промышленного изготовления[7].

Очередным толчком к развитию теоретических положений в области маскировки послужила война ВС США во Вьетнаме. С учетом культурных и национальных отличий народов Юго-Восточной Азии, а также географических и природно-климатических особенностей региона были уточнены методы и порядок реализации мер по дезинформации, легендированию мест дислокации и скрытию районов расположения войск, а также усовершенствованы палитра красок и схемы окрашивания основных образцов ВВСТ[8,9,10] (рис. 2).

В отношении демонстративных действий выдвигалось жесткое требование к их систематичности. По сути, предполагалось разрабатывать еще одну «выдуманную» операцию (бой) с соответствующими решениями, планами и действиями, которые противник должен принять за истинные. Для этого силам и средствам, выделенным для демонстрации, предписывалось активно перемещаться, проводить атаки, наносить удары по второстепенным объектам и тем самым отвлекать внимание противника от районов и направлений действий главных сил. Так, американское командование в конце 1966 — начале 1967 года в целях ослабления внимания войск Национального фронта освобождения Южного Вьетнама организовало и успешно провело в дельте р. Меконг отвлекающую десантную операцию[11].

Очередной этап развития маскировки в ВС США (середина 80-х — начало 90-х годов XX века) характеризовался поиском решений по скрытию и имитации войск в условиях использования противником оптических, телевизионных, радиолокационных и сейсмоакустических средств разведки, а также приборов, позволяющих обнаруживать технику и объекты в ультрафиолетовом диапазоне спектра электромагнитных волн. Разведывательные органы потенциальных противников интенсивно оснащались подобными средствами, а их совместное применение сокращало время поиска, обнаружения и идентификации целей (объектов), а также повышало достоверность полученных разведданых.

С учетом данного фактора **в ВС США были определены три базовых принципа маскировки:**

• правильный и продуманный выбор мест расположения войск и объектов с учетом особенностей и скрывающих свойств местности;

• умелое использование естественных и искусственных материалов как для скрытия войск и объектов, так и для создания ложных целей;

• строгое и непрерывное выполнение организационных мероприятий по соблюдению маскировочной дисциплины: светомаскировка, минимизация перемещений в светлое вре-

Рис. 2. БТР М113 с камуфлирующей окраской для действий в джунглях

мя суток, особенно на переднем крае, использование на технике звуковых глушителей и др.

В этот период маскировку в ВС США перестают считать деятельностью только тактических подразделений и начинают включать в содержание планов и действий войск на оперативном уровне. Для подготовки решений по маскировке и разработки соответствующих планов в штабах создаются специальные рабочие органы во главе с офицером оперативного отдела (отделения). При этом особое внимание уделяется достижению максимальной правдоподобности и реалистичности обманных действий. В качестве главной цели реализации комплекса мероприятий по скрытию и имитации принимается повышение живучести войск и объектов. Основными критериями оценки их эффективности становятся скорость и качество решения соответствующих задач[12].

Ввиду существенного роста масштабов маскировочных мероприятий они преимущественно выполняются силами скрываемых подразделений. Главным руководящим документом по маскировке в этот период служит изданный в 1990 году ***устав FM 20-3 «Скрытие»***, в котором излагаются особенности скрытия ВВСТ в обороне, наступлении, на марше, в том числе с использованием принятого на тот момент на снабжение нового облегченного маскировочного комплекта *LCSS* (легкая система маскировочных экранов) (рис. 3). Отдельным пунктом в уставе даны рекомендации по скрытию особо важных объектов: командных пунктов, подразделений подвоза ядерных боеприпасов, пусковых установок и т. п.

Рис. 3. Скрытие САУ М106 «Паладин» с использованием маскировочного комплекта LCSS и естественной растительности

Наряду с этим издается Технический бюллетень ***TB 43-0209 «Окрашивание военной техники, имущества и оборудования»***, которым в очередной раз уточняются варианты окраски ВВСТ сухопутных войск. Положения данного документа остаются актуальными по настоящее время[13].

Помощь подразделениям в организации маскировки оказывает инженер части или соединения. Для планирования и руководства маскировочными работами, обучения личного состава способам скрытия и имитации, наблюдения за маскировочной дисциплиной, подготовки и использования ложных сооружений и макетов привлекаются и специальные подразделения — инженерно-маскировочные роты[14].

Война в Персидском заливе (1990—1991) вскрыла существенные недостатки и упущения в подготовке командного состава ВС США по вопросам планирования маскировки. Проявилась неготовность личного состава качественно проводить мероприятия скрытия в условиях пустын-

ной местности — сказались отсутствие опыта, соответствующих технических средств маскировки и подручных материалов (рис. 4). Победа в очередной раз была достигнута исключительно за счет массированного применения авиации (в том числе беспилотной) и высокоточного оружия[15,16,17].

Рис. 4. Передвижение боевой техники ВС США без соблюдения мер скрытия в ходе войны в Персидском заливе (1990—1991)

Допущенные просчеты частично планировалось исправить путем дезинформации противника. Так, предусматривалось создавать и развертывать группировки войск (сил) в регионе под легендой обеспечения контроля соблюдения международных санкций, выполнения других внешнеполитических обязательств и защиты мирных жителей, отстаивающих свои права.

Параллельно с сокрытием планов предстоявших военных действий и сроков их начала через специально созданные группы журналистов и средства массовой информации распространялись ложные сведения о неполной готовности американских войск к операции, переносе сроков ее начала и т. п. На самом деле агрессию предусматривалось развязать до завершения стратегического развертывания ограниченным составом сил с последующим их наращиванием в ходе боевых действий, что стало для противника полной неожиданностью.

Достижение внезапности с использованием подобной военной хитрости обеспечивалось также в операциях ВС США и НАТО «Союзная сила», «Несгибаемая свобода», «Свобода Ираку» и «Объединенный защитник»[18,19].

Однако, несмотря на все ухищрения политического, дипломатического и военного характера по сохранению в тайне замыслов и сроков начала агрессии, а также колоссальные материальные и финансовые затраты, американские военные специалисты признают тот факт, что выполнение противником мероприятий маскировки даже в ограниченном объеме с использованием простых и дешевых средств негативно влияло на информационную осведомленность органов управления и снижало эффективность ударов, в том числе высокоточным оружием.

Итоги проведенных операций продемонстрировали важность и нужность маскировки, необходимость адаптации всех ее компонентов к условиям применения, а также разработки соответствующих технических средств, способов и приемов их использования. **Парадигмой развития маскировки становится переход от пассивных масштабных**

шаблонных действий к целенаправленному активному навязыванию противнику ложного или искаженного представления об обстановке, составе, характере и содержании действий своих войск, расположении и предназначении объектов.

Дезинформация как одно из средств достижения победы превращается в неотъемлемую составляющую обеспечения военных действий. Начиная с 1994 года ее роль в системе вооруженной борьбы неуклонно растет, а доля соответствующих мероприятий в информационном противоборстве различного уровня и масштаба существенно повышается. **Дезинформация выделяется в отдельное научно-практическое направление со следующими целевыми установками:**

- придать действиям своих органов управления и войск двусмысленность;
- внести путаницу в понимание противником смысла предпринимаемых действий;
- заставить противника неверно оценить сильные и слабые стороны противостоящей группировки войск (сил), нерационально распределить людские, финансовые и материальные ресурсы, сосредоточить войска на второстепенных направлениях и участках;
- вынудить противника заблаговременно раскрыть свои намерения[20,21].

По мере расширения номенклатуры технических средств, способов и вариантов их применения трансформировались принципы дезинформации, общие и частные подходы к навязыванию противнику ложных сведений и особенности выполнения мероприятий в зависимости от поставленных целей, уровня решаемых задач и объемов привлекаемых ресурсов.

В настоящее время дезинформация в ВС США представляет собой комплекс мероприятий, проводимых в целях введения руководящего состава противника (командиров формирований регулярных войск и незаконных вооруженных формирований, главарей экстремистских (террористических) организаций) в заблуждение путем формирования и доведения через его разведывательные органы ложной информации и убеждения в ее достоверности. Проводится на всех уровнях от стратегического до тактического[22].

Актуальные положения в области дезинформации раскрываются в следующих руководящих документах ВС США:

- Инструкция министра обороны 3604.01 «Мероприятия дезинформации в Министерстве обороны США» (2013);
- Инструкция Комитета начальников штабов (КНШ) 3211.01 «Принципы дезинформации» (2015);
- Наставление КНШ *JP 3-13.4* «Дезинформация» (2019);
- на межвидовом уровне действует документ «Приемы и способы дезинформации в операции (на ТВД)» (2010);
- в сухопутных войсках принят устав *FM 3-13.4* «Действия формирований по обеспечению дезинформации» (2019).

В перечисленных документах отмечается, что успешная реализация дезинформации возможна исключительно при соблюдении принципов (сосредоточенность, целеустремленность, централизация планирования и управления, безопасность, согласованность, интеграция) алгоритмов планирования, а также при своевременном и качественном выполнении намеченных действий в рамках разработанной легенды прикрытия.

Принятая в ВС США методология планирования обманных действий (*Military Deception Planning*

Methodology) базируется на системе представлений о причинно-следственных связях процессов информационного и физического характера, протекающих между противостоящими сторонами. Данные процессы характеризуются непрерывностью и цикличностью (рис. 5).

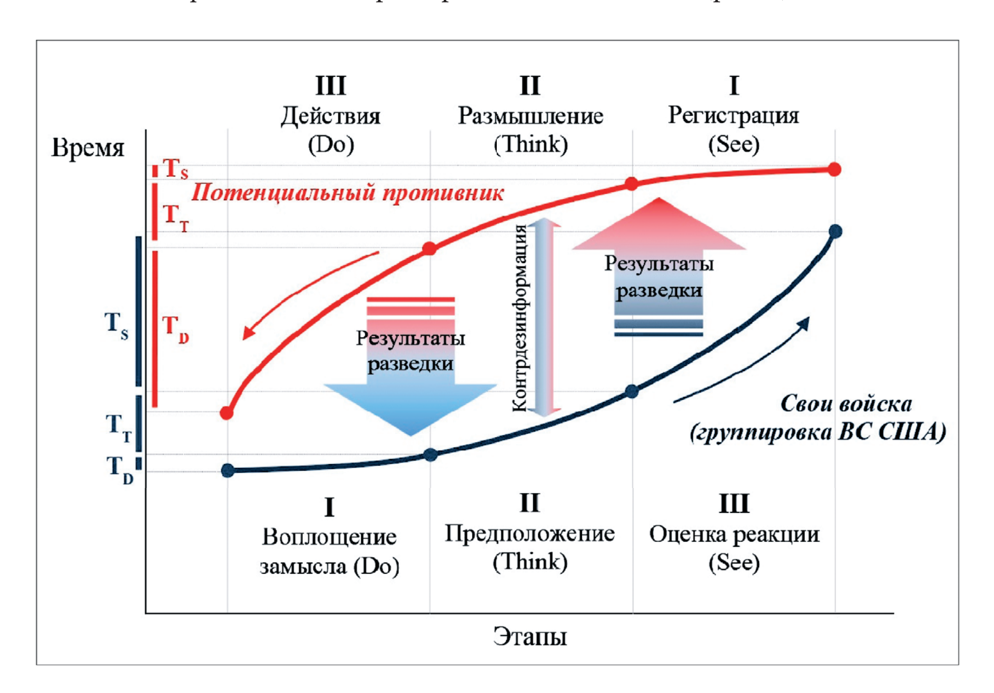


Рис. 5. Цикл действий противоборствующих сторон в рамках дезинформации

Как показано на рисунке, в типовом цикле действий своих войск (группировка ВС США) установлена последовательность «воплощение замысла — предположение — оценка реакции».

На первом этапе данного цикла создаются условия для того, чтобы разведорганы противника зарегистрировали обманные действия и/или получили ложную информацию, т. е. ему дается «пища» для размышлений. Опережение противника в навязывании ему дезинформации обеспечивает удержание стратегической инициативы.

Второй этап носит прогнозно-аналитический характер. Оцениваются возможные варианты ответных шагов противника: корректировка планов боевого применения, принятие нового решения или отказ от действий. Формируется представление о том, что может предпринять противник в результате выводов, основанных на ложных сведениях.

На третьем этапе оценивается степень соответствия действий войск противника замыслу, заложенному в легенду дезинформации на этапе планирования.

При этом предполагается, что противник будет реагировать на дезинформацию в следующей последовательности: «регистрация — размышление — действия или отказ от них». В качестве аксиомы принимается его слабая информационная осведомленность, и, как результат, неспособность вести свою «игру», что неизбежно ведет к подчинению выдвигаемым условиям.

Нелинейная зависимость этапов по времени — следствие особенностей выполнения мероприятий на каждом из них. Действия разведывательных органов любой из сторон, а также выполнение мероприятий по контрдезинформации могут сократить время, отводимое на этап, либо исключить необходимость перехода к следующему.

Обманные действия в ВС США реализуются следующими способами:

• *ложные маневры* — осуществляются в целях отвлечения и/или дезориентирования противника относительно направлений сосредоточения основных усилий, места и времени нанесения главного удара. Выполняются силами реальных воинских формирований, которые тем не менее не исключаются из плана боевого применения войск;

• *демонстративные действия* — преднамеренный показ определенной деятельности воинских формирований либо элементов боевого порядка без огневого контакта в целях введения противника в заблуждение относительно характера истинных действий войск и их намерений. Проводятся силами специальных демонстративных групп;

• *хитрость* — проведение обманных мероприятий в целях вынудить противника сосредоточить усилия разведки на второстепенных и ложных направлениях;

• *показ* — воспроизведение демаскирующих признаков, присущих другим, менее важным со стратегической (оперативной, тактической) точки зрения объектам в рамках легенды дезинформации. Реализуется путем применения масок-принадлежностей, преднамеренного небрежного выполнения мероприятий скрытия, нарушения требований по скрытому управлению войсками и светомаскировке[23,24].

Приемы дезинформации зависят от таких переменных факторов, как время, количество и качество выделенных на это сил и средств. Действиям предшествует оценка вероятности достижения поставленной цели, риски и угрозы срыва выполнения задач. Исходя из обстановки подбирается такой комплекс приемов, реализация которых в установленной последовательности позволит убедить противника в реалистичности активности разведывательных действий на ложном направлении, учений и испытаний, функционирования войск в ложных районах сосредоточения.

Таким образом, развитие теории и практики маскировки в ВС США представляет собой закономерный процесс эволюции данного раздела военной науки, базирующийся на опыте применения войск (сил) в современных военных конфликтах и своевременном реагировании на появление новых средств вооруженной борьбы. Система планирования и выполнения задач маскировки не является статичной, а совершенствуется в направлении комплексного и «адресного» применения разнородных сил средств в интересах повышения живучести своих войск и объектов при одновременном введении противника в заблуждение.

Так, уже в ближайшее время следует ожидать корректировки архитектуры маскировки, смыслового содержания и логического наполнения терминов и определений, используемых в области дезинформации, которая занимает центральное место в системе информационного противоборства. Наряду с этим активизируются усилия по созданию и оснащению войск новыми техническими средствами скрытия, ими-

тации и дезинформации в целях существенного повышения эффективности мероприятий защиты войск и объектов.

В связи с этим вопросы оценки и прогнозирования тенденций развития маскировки и способов выполнения соответствующих задач в ВС США имеют важное значение и должны учитываться при планировании строительства, подготовки и применения ВС России как на современном этапе, так и в военных конфликтах будущего.

ПРИМЕЧАНИЯ

[1] Engineer Field Manual Volume II Military Engineering (Tentative) Part Two Defensive Measures. Washington: Under the Direction of the Chief of Engineers, 1932. P. 258.

[2] *Caddell W.J.* Deception 101 — Primer on Deception. Military History at North Carolina State University, 2004. P. 26.

[3] *Latimer J.A.* Deception in War. London: Thistle Publishing, 2015. 257 p.

[4] Операция «Камуфляж»: как американцы заставили исчезнуть свои военные заводы // Военно-политическое обозрение. URL: https://www.belvpo.com/90997.html/ (дата обращения: 01.11.2021).

[5] *Hartcup G.P.* Camouflage. A History of Concealment and Deception in War. New York: 1980. 156 p.

[6] FM 5-23 Field Decoy Installations. Department of the Army, 1956. 196 p.

[7] FM 5-20 Camouflage Basic Principles and Field Camouflage. Headquarters, Department of the Army, 1959. 254 p.

[8] FM 5-20 Camouflage. Headquarters, Department of the Army, 1968. 105 p.

[9] Technical Bulletin 43-0147 Color, Marking and Camouflage Patterns Used on Military Equipment. Headquarters, Department of the Army, 1975. 163 p.

[10] Training Circular 5-200 Camouflage Pattern Painting. US Army Engineer School, 1975. 20 p.

[11] *Иванов В.С.* Способы дезинформации противника по мнению военных специалистов НАТО // Зарубежное военное обозрение. 1976. № 7. С. 58.

[12] FM 90-2 Battlefield Deception. Headquarters, Department of the Army, 1988. 176 p.

[13] FM 20-3 Camouflage. Headquarters, Department of the Army, 1990. 81 p.

[14] *Гришин С.В., Цапенко Н.Н.* Соединения и части в бою. М.: Воениздат, 1985. С. 102—105.

[15] *Валецкий О.В., Гирин А.В., Маркин А.В., Неелов В.М.* Уроки Ирака. Тактика, стратегия и техника в Иракских войнах США. М.: Издатель Воробьев А.В., 2015. 212 с.

[16] Война в Персидском заливе. М.: Воениздат, 1993. С. 210.

[17] *Кларк У.* Как победить в современной войне. М.: Альпина Бизнес Букс, 2004. 271 с.

[18] *Владимиров В.Н.* Наземная операция ВС США и их союзников против Ирака // Зарубежное военное обозрение. 2004. № 1. С. 63.

[19] *Марков К.А.* Маскировка в военных конфликтах конца XX — начала XXI века // Военно-исторический журнал. 2018. № 6. С. 24—28.

[20] JP 3-13.4 Military Deception. Joint Chiefs of Staff, 2012. 81 p.

[21] *Ramana J.R.* Introduction to Camouflage and Deception. New Delhi: Defence Research & Development Organisation, 1999. 354 p.

[22] DOD Dictionary of Military and Associated Terms. Department of Defense, 2021. 366 p.

[23] JP 3-13.4 Military Deception. Joint Chiefs of Staff, 2017. 108 p.

[24] *Быстров В.Н., Крысанов М.Ф.* Некоторые особенности военной дезинформации за рубежом // Зарубежное военное обозрение. 2001. № 7. С. 11—14.

Выдающиеся деятели военной науки

22 ИЮНЯ 2022 года — 100 лет со дня рождения активного участника Великой Отечественной войны, доктора военных наук, профессора, заслуженного деятеля науки РФ, почетного профессора Военной академии имени М.В. Фрунзе, действительного члена Академии военных наук и Международной академии информатизации генерал-майора в отставке Ивана Николаевича Воробьёва.

Иван Николаевич родился в селе на Тамбовщине. После учебы в школе поступил в педагогическое училище, которое окончил с отличием. Поработав учителем, он поступил в Таллинское военное пехотное училище. Там и застала его война.

После досрочного выпуска Иван Николаевич вступил в должность командира пехотного взвода, стал воевать в районе Пскова и Великого Новгорода. До весны 1942 года получил несколько ранений. Пройдя по фронтовым огненным дорогам в составе Северо-Западного и 2-го Прибалтийского фронтов, И.Н. Воробьёв закончил войну командиром стрелкового батальона. За отличия в боях награжден тремя орденами, в том числе орденом Красного знамени.

После окончания Великой Отечественной войны Иван Николаевич продолжил службу. Как грамотный перспективных офицер он был направлен на учебу в прославленную Военную академию имени М.В. Фрунзе, которую окончил в 1950 году с отличием и золотой медалью.

Иван Николаевич проявил себя и как пытливый военный исследователь. Он защитил диссертацию на соискание ученой степени кандидата военных наук, стал преподавателем в академии на основной кафедре — кафедре тактики. Продолжая научно-педагогическую деятельность, Иван Николаевич дерзнул на написание докторской диссертации. В соответствии с установленным порядком он написал рапорт, а тему в то время, как, впрочем, и сейчас, утверждал Главнокомандующий Сухопутными войсками. Тема диссертации звучала так — «Наступление мотострелковой дивизии в горах». Главнокомандующий Сухопутными войсками Маршал Советского Союза В.И. Чуйков — один из героев Сталинграда и самых мужественных и строгих полководцев, написал примерно вот такую резолюцию: «назначить полковника И.Н. Воробьева на должность заместителя командира дивизии в Ленинакан, ему же подготовить опытное учение по теме диссертации. Учение буду проверять лично». Вот так разрабатывались диссертации в то время!

Иван Николаевич с честью выдержал и служебную, и научную нагрузки, а присутствующий на учении Маршал Советского Союза В.И. Чуйков дал высокую оценку как учению, так и диссертации. Впоследствии соискатель защитил докторскую диссертацию и на диссертационном совете академии. После защиты диссертации И.Н. Воробьёва назначили заместителем начальника кафедры тактики, которую возглавлял другой легендарный ученый академии — В.Г. Резниченко, впоследствии генерал-лейтенант, заместитель начальника академии по учебной и научной работе. Именно из недр этой кафедры вышла главная фундаментальная книга Вооруженных Сил СССР, которую изучали офицеры всех специальностей — «Общая тактика». Во времена СССР книга выдержала 22 издания. В настоящее время она официально издана в Белоруссии и других странах — бывших республиках СССР, а также во многих странах Африки, Латинской Америки и Азии. Неофициально книгу переиздали и тщательно изучали и изучают наши западные «партнеры».

В 1964 году Министром обороны СССР стал Маршал Советского Союза А.А. Гречко. Он потребовал, чтобы помощником у него был один из ведущих военных ученых. После долгих поисков на эту должность был рекомендован доктор военных наук полковник И.Н. Воробьёв, благодаря которому А.А. Гречко стал очень уважительно относиться в военной науке и дал указание создать при Министре обороны группу военных ученых, которая известна как Группа информации.

В 1987 году, послужив при министрах обороны СССР Д.Ф. Устинове и С.Л. Соколове, Иван Николаевич в возрасте 65 лет был уволен в запас. Наконец-то он мог полностью отдаться военной науке в родной академии, где он как лично, так и в соавторстве, написал десятки книг и научных статей.

Особо следует выделить труд, который может быть охарактеризован как непревзойденный и, не побоюсь сказать, гениальный в военной науке, — «Принципы общевойскового боя». Вся квинтэссенция военной науки в этом труде! Его можно поставить в один ряд с творениями многих других корифеев военной науки.

Ивана Николаевича можно считать основоположником новейшей современной отрасли военной науки — военной футурологии. Он первым в 1998 году написал и издал военно-теоретический труд «О военной футурологии», который был дважды дополнен и в соавторстве переиздан. Данная работа также получила высочайшую оценку военно-научного сообщества страны и за ее пределами.

Не меньшим научным богатством И.Н. Воробьёв считал своих учеников. В качестве научного руководителя он подготовил десятки кандидатов наук, а научного консультанта — многих докторов наук. Следует отметить, что военные ученые других академий и научно-исследовательских организаций получали профессиональные консультации и советы Ивана Николаевича.

И.Н. Воробьёв активно работал в Академии военных наук России, возглавлял одну из секций отделения «Военное искусство». Его труды неизменно получали высокую оценку ученых академии и справедливо были отмечены премиями имени А.В. Суворова и А.А. Свечина.

Многие годы Иван Николаевич плодотворно сотрудничал с журналом «Военная Мысль». Впервые он выступил на его страницах с публикацией в 1957 году (№ 10). С тех пор до конца своей жизни редко в какой год мы не найдем его фамилии среди авторов журнала. Перу Ивана Николаевича принадлежит более 150 статей. Их тематика обширна — от тактики до стратегии и общих проблем военной науки. Его статьи: «Новое оружие — новая тактика», «Какие мобильные силы нам нужны», «Какие войны угрожают нам в будущем веке», «Почему тактика оказалась в застое», «От современной тактики к тактике сетецентрических действий» — признаны лучшими в журнале и удостоены премии Министерства обороны.

В конце 1990-х годов важность дальнейшего совершенствования вопросов теории и практики применения соединений, частей, подразделений всех родов войск (сил) в бою приобрела острую актуальность. На то время И.Н. Воробьёв закончил работу над учебником «Тактика — искусство боя». С согласия видного военного теоретика редакция в 2002—2003 годах опубликовала в рубрике «И.Н. Воробьёв. О тактике» основные мысли ученого, в которых сконцентрирован его богатый научный и педагогический опыт. В 2004 году редакцией был выпущен специальный сборник с аналогичным названием.

Иван Николаевич был прекрасным человеком с щедрой широчайшей душой, отзывчивым сердцем — настоящим Русским Человеком и Учителем.

Отмечая справедливость известной фразы «Незаменимых нет», подчеркну справедливость ее продолжения — «…но есть неповторимые»! Именно таким был и останется в нашей памяти Иван Николаевич Воробьёв! Ведь память — это благодарность сердца!

Член редакционной коллегии журнала «Военная Мысль»
генерал-майор запаса В.В. КРУГЛОВ, доктор военных наук

ИНФОРМАЦИЯ ОБ АВТОРАХ
INFORMATION ABOUT THE AUTHORS

КАЛГАНОВ Виктор Александрович, вице-адмирал, кандидат технических наук, доцент / Viktor KALGANOV, rear admiral, Cand. Sc. (Tech.), assistant professor.

РЫЖОВ Геннадий Борисович, генерал-майор, доктор военных наук, профессор, советник Российской академии ракетных и артиллерийских наук / Gennady RYZHOV, major general, D. Sc. (Mil.), professor, adviser at the Russian Academy of Missile and Artillery Sciences.
E-mail: salamandra.n5@mail.ru

СОЛОВЬЁВ Игорь Владимирович, капитан 1 ранга в отставке, доктор технических наук, профессор / Igor SOLOVYEV, captain 1st rank (ret.), D. Sc. (Tech.), professor.
E-mail: i.v.soloviev54@mail.ru

СОКОЛОВ Виктор Николаевич, вице-адмирал / Viktor SOKOLOV, rear admiral.

ХАРЖАВИН Александр Викторович, полковник запаса, кандидат военных наук, доцент / Alexander KHARZHAVIN, colonel (res.), Cand. Sc. (Mil.), assistant professor.
Телефон / Phone: 8 (812) 431-91-59.

НОГИН Роман Олегович, генерал-майор, кандидат военных наук / Roman NOGIN, major general, Cand. Sc. (Mil.).
Телефон / Phone: 8 (495) 524-07-01.

ХАЧАТРЯН Артак Ваникович, полковник запаса, кандидат военных наук / A.V. KHACHATRYAN, colonel (res.), Cand. Sc. (Mil).

ШИЛОНОСОВ Артем Владимирович, подполковник, кандидат педагогических наук / A.V. SHILONOSOV, lieutenant colonel, Cand. Sc. (Educ.).

УЛАНОВ Александр Сергеевич, подполковник запаса, кандидат технических наук, старший научный сотрудник АО «Концерн воздушно-космической обороны «Алмаз-Антей» / Alexander ULANOV, lieutenant colonel (res.), Cand. Sc. (Tech.), senior researcher at Almaz-Antei Aerospace Defense Concern.
E-mail: bab5@bk.ru

СИМОНОВ Андрей Дмитриевич, генерал-майор / Andrei SIMONOV, major general.
Телефон / Phone: 8 (495) 498-66-44.

ВОРОБЬЁВ Игорь Геннадьевич, полковник, кандидат военных наук, доцент / Igor VOROBYEV, colonel, Cand. Sc. (Mil.), assistant professor.
E-mail: viggspb@mail.ru

РОМАНОВ Виктор Михайлович, полковник / Viktor ROMANOV, colonel.

ПОПОВА Мария Александровна, майор / Maria POPOVA, major.

МИХАЙЛОВ Вадим Валерьевич, генерал-майор / Vadim MIKHAILOV, major general.

СЕРГЕЕВ Владимир Игоревич, подполковник, доктор технических наук / Vladimir SERGEYEV, lieutenant colonel, D. Sc. (Tech.).
E-mail: sergeev_v@bk.ru

ФИЛИН Дмитрий Александрович, майор / Dmitry FILIN, major.

ГЛУХОВ Евгений Александрович, полковник юстиции, кандидат юридических наук, доцент / Yevgeny GLUKHOV, colonel of justice, Cand. Sc. (Law), assistant professor.
E-mail: evgenijgluhov@yandex.ru

ГАРБУК Сергей Владимирович, кандидат технических наук, старший научный сотрудник, директор по научным проектам НИУ «Высшая школа экономики / Sergei GARBUK, Cand. Sc. (Tech.), senior researcher, director of research projects at the National Research University "Higher School of Economics".
E-mail: garbuk@list.ru

БЕЖЕНЦЕВ Алексей Юрьевич, полковник, кандидат технических наук / Alexei BEZHENTSEV, colonel, Cand. Sc. (Tech).

ПОЛЯКОВ Артем Евгеньевич, майор / Artyom POLYAKOV, major.

ТУМАКОВ Владимир Матвеевич, подполковник в отставке / Vladimir TUMAKOV, lieutenant colonel (ret.).

ЗЕЛЕНОВ Анатолий Васильевич, полковник запаса, кандидат военных наук, доцент / Anatoly ZELENOV, colonel (res.), Cand. Sc. (Mil.).
Email: anatoliigreen@mail.ru

ВДОВИН Александр Владимирович, полковник запаса, кандидат военных наук, доцент, научный сотрудник института управления / Alexander VDOVIN, colonel (res.), Cand. Sc. (Mil.), assistant professor, researcher at the Management Institute.
Email: vdovinav@mail.ru

ЛЕВЕНТОВ Николай Николаевич, полковник в отставке, кандидат военных наук, старший научный сотрудник НИЦ / Nikolai LEVENTOV, colonel (ret.), Cand. Sc. (Mil.), senior researcher at the Research Center.

АЛЁШЕЧКИН Николай Дмитриевич, полковник в отставке, кандидат технических наук, профессор, старший научный сотрудник НИЦ / Nikolai ALESHECHKIN, colonel (ret.), Cand. Sc. (Tech.), professor, senior researcher at the Research Center.

АНАСТАСИН Александр Валентинович, полковник в отставке, кандидат военных наук, доцент, старший научный сотрудник НИЦ / Alexander ANASTASIN, colonel (ret.), Cand. Sc. (Mil.), assistant professor, senior researcher at the Research Center.

СИДОРОВ Михаил Петрович, полковник, в/ч 45880 / M.P. SIDOROV, colonel, Unit 45880.

ОВСЯННИКОВ Сергей Николаевич, майор, в/ч 45880 / S.N. OVSYANNIKOV, major, Unit 45880.

ГОРОХОВ Роман Юрьевич, кандидат технических наук, старший научный сотрудник НИО / Roman GOROKHOV, Cand. Sc. (Tech.), senior researcher at research section.

Учредитель: Министерство обороны Российской Федерации
Регистрационный № 01974 от 30.12.1992 г.

Главный редактор С.В. Родиков.
В подготовке номера принимали участие:
М.В. Васильев, В.Н. Каранкевич, П.В. Карпов, А.Ю. Крупский
В.Д. Кутищев, А.Н. Солдатов, В.Н. Щетников, А.И. Яценко,
Л.В. Зубарева, Е.Я. Крюкова, Г.Ю. Лысенко,
Л.Г. Позднякова, Н.В. Филиппова, О.Н. Чупшева.
Компьютерная верстка: И.И. Болинайц, Е.О. Никифорова.

Сдано в набор 22.06.2022 Подписано к печати 20.07.2022
Формат 70×108 1/16 Бумага офсетная 10 п.л.
Печать офсетная Тираж 1657 экз. Заказ 2917-2022

Журнал издается ФГБУ «РИЦ «Красная звезда» Минобороны России
Адрес: 125284, г. Москва, Хорошёвское шоссе, д. 38.
Тел: 8(495)941-23-80, e-mail: ricmorf@yandex.ru
Отдел рекламы — 8(495)941-28-46, e-mail: reklama@korrnet.ru

Отпечатано в АО «Красная Звезда»
Адрес: 125284, г. Москва, Хорошёвское шоссе, д. 38.
Тел: 8(499)762-63-02.
Отдел распространения периодической печати — 8(495)941-39-52.
Цена: «Свободная».

НАШИ ПОЗДРАВЛЕНИЯ

ДЕНЬ ВОЗДУШНО-ДЕСАНТНЫХ ВОЙСК

2 АВГУСТА профессиональный праздник десантников — День Воздушно-десантных войск. В этот день на учениях Московского военного округа впервые было выброшено на парашютах подразделение десантников для выполнения тактической задачи в тылу противника. Возникнув как мобильный род войск в 1930 году, «крылатая пехота» получила боевое крещение в 1939-м — в боях на реке Халхин-Гол, где было активно задействовано 212 воздушно-десантных бригад.

В годы Великой Отечественной войны Воздушно-десантные войска с честью выдержали суровые испытания, проявив в боях героизм, мужество и отвагу, за что всем воздушно-десантным соединениям было присвоено звание гвардейских. Затем были Афганистан, Северный Кавказ, миротворческие операции. И всюду воины-десантники с достоинством и честью выполняли поставленные задачи, демонстрируя высокую профессиональную подготовку, массовый героизм, взаимовыручку и самопожертвование.

Сейчас Воздушно-десантные войска являются военной элитой наших Вооруженных Сил. Лозунг десантников «Никто, кроме нас» наглядно демонстрирует особый морально-боевой кодекс и особую ответственность «голубых беретов» за судьбу нашего Отечества.

ДЕНЬ ЖЕЛЕЗНОДОРОЖНЫХ ВОЙСК

ПЕРВОЕ упоминание о военно-железнодорожном подразделении произошло 6 августа 1851 года, когда император Николай I ратифицировал «Положение о составе Санкт-Петербургско-Московской железной дороги». Были созданы военно-рабочие, кондукторские и телеграфные роты (позднее команды и батальоны) общей численностью более 4000 человек.

Сегодня военнослужащие железнодорожных войск осуществляют строительство, эксплуатацию, восстановление железнодорожного полотна, предназначенного для военных перевозок, а также выполняют другие специальные задачи, в том числе участвуют в ликвидациях последствий чрезвычайных ситуаций.

Редакционная коллегия и редакция журнала «Военная Мысль» поздравляют командование, личный состав, ветеранов Воздушно-десантных войск и Железнодорожных войск с профессиональными праздниками! Пусть вам всегда сопутствуют удача и успех. Желаем крепкого здоровья, мирного неба, благополучия и дальнейших успехов в деле укрепления обороноспособности нашей Отчизны.

Внимание!

Полная и сокращенная версии журнала размещаются на официальном сайте редакции — http://vm.ric.mil.ru; научные материалы — на сайте Научной электронной библиотеки — http://www.elibrary.ru; e-mail: ric_vm_4@mil.ru

Подписку на журнал на 2-е полугодие 2022 года можно оформить по каталогу АО «Почта России» по индексу П5907 в любом почтовом отделении, кроме Республики Крым и г. Севастополя; Объединенному каталогу «Пресса России» через ОАО «АРЗИ» по индексу 39891 в почтовых отделениях Республики Крым и г. Севастополя; интернет-каталогу «Пресса России», индекс Э39891 для подписчиков всех регионов; интернет-каталогам агентств на сайтах: www.podpiska.pochta.ru, www.akc.ru, www.pressa-rf.ru; заявке на e-mail: kr_zvezda@mail.ru с личным получением в АО «Красная Звезда», г. Москва, или доставкой бандеролью.

ISSN 0236-2058 Военная Мысль. 2022. № 8. 1—160